Arithmétrique en différentes caractéristiques

Pierre Jalinière

UNIVERSITÉ PIERRE ET MARIE CURIE

THÈSE

Présentée pour obtenir

LE GRADE DE DOCTEUR DE
L'UNIVERSITÉ PIERRE ET MARIE
CURIE

École Doctorale 386 Sciences Mathématiques de Paris Centre

par

Pierre JALINIÈRE

Arithmétique en différentes caractéristiques

Soutenue le 4 juillet 2016 devant la Commission d'examen:

M.	Laurent CLOZEL	
M.	Mladen DIMITROV	
M.	Pierre-Vincent KOSELEFF	
M.	Reynald LERCIER	(Rapporteur)
Mme	Ariane MÉZARD	(Directrice de thèse)
M.	Fabrice ROUILLIER	

Rapporteurs:

M.	Jean-Marc Couveignes
M.	Reynald Lercier

Thèse préparée à
Institut de Mathématiques de Jussieu Paris Rive Gauche
Université Pierre et Marie Curie
4 Place Jussieu
75005 Paris

Abstract

Cette thèse comporte trois volets indépendants en cryptographie, en théorie de Hodge p-adique et en analyse numérique.

La première partie consiste en l'étude d'algorithmes performants de résolution du logarithme discret . La résolution du logarithme discret consiste à déterminer les exposants d'une famille fixée de générateurs dans la décomposition des éléments du groupe. Dans le cas des groupes multiplicatifs d'un corps fini, la complexité des calculs dépendent de la taille - dite de petite, moyenne ou grande caractéristique- de la caractéristique du corps dans lesquels on effectue les calculs.
Nous présentons différents algorithmes dans chacune des caractéristiques (petite, moyenne ou grande) en précisant quel est l'algorithme le plus performant dans chacun des cas.

La seconde partie s'inscrit dans le contexte du programme de Langlands p-adique. Nous présentons une généralisation de l'un des outils centraux de la théorie, les modules de Breuil-Kisin.

La troisième partie est un travail initié lors de la treizième SEME, Semaine d'Etudes Maths Entreprises organisée par l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société (AMIES). L'Institut Français du Pétrole et des Energies Nouvelles nous a soumis un problème de résolution numérique d'un système d'équations modélisant la désorption d'un gaz de schiste en une dimension. Nous proposons plusieurs schémas du premier ordre recourant à un traitement implicite de l'équation de relaxation.

Abstract

In this thesis, we present three independent works in cryptography, p-adic Hodge theory and Numerical analysis.

First we present several algorithms to solve the discrete logarithm in several characteristic finite fields. We are particularly interested with the determination of classes of polynomial functions with small coefficients.

The second part of the thesis deals with one of the major object of p-adic Hodge theory. We present a multi-variable version of Breuil-Kisin modules where the Lubin-Tate tower replaces the classical cyclotomic tower.

He third part proposes two numerical schemes for the modelisation of desorption of shale gaz.

Remerciements

Mes remerciements vont en premier lieu à ma directrice de thèse, Ariane Mézard pour sa patience, son accompagnement et son enthousiasme à me faire découvrir des mathématiques et des domaines nouveaux durant ces quatre années. Je remercie également Jean-Marc Couveignes et Reynald Lercier de me faire l'honneur d'être rapporteurs de ma thèse. Les mathématiques de Reynald lercier ont guidé mon travail. Je lui en suis reconnaissant. Que soient remerciés Laurent Clozel, Mladen Dimitrov, Pierre-Vincent Koseleff, Fabrice Rouillier, membres de mon jury. J'ai découvert les mathématiques contemporaines et particulièrement l'arithmétique avec laurent Clozel. C'était à Orsay, il y a plus de dix ans aujourd'hui. Je garde présent le souvenir de sa disponibilité pour l'étudiant que j'étais. Mladen Dimitrov a dirigé mon mémoire de Master. J'ai découvert grâce à lui le pan modulaire de la théorie des nombres. C'était un nouvel univers. Il m'en a montré les tous premiers aspects.

Les différentes parties du présent manuscrit sont le fruit de plusieurs collaborations. La partie cryptographie doit ainsi beaucoup à Cécile Pierrot, étudiante en thèse au laboratoire d'informatique de Paris VI, que je remercie ici pour sa disponibilité et ses idées fructueuses. Antoine Joux a veillé de loin avec bienveillance sur la pertinence de nos travaux. Eugen Hellmann a participé à la création de la partie proprement arithmétique du présent travail. Enfin la partie modélisation est un travail commun initié lors d'un séminaire de doctorant à Nantes. Je remercie ici tous les membres de notre petit groupe Victor Vilaça Da Rocha, Roberta Tittarelli, Richard Sambilason Rafemanana, Victor Michel-Dansac et Benjamin Couéraud.

Pour conclure, je pense à mes parents, mes frères Hugo et Baptiste, mon grand père Georges Jalinière, ma belle sœur Aurore, mon petit neveu Gaspard et mes amis David, Kenza, Nicolas, qui m'ont tout le temps de cette thèse soutenu et accompagné, même dans les moments difficiles, je les en remercie tous.

Contents

Introduction

Cette thèse comporte trois volets indépendants en cryptographie, en théorie de Hodge p-adique et en analyse numérique.

La première partie consiste en l'étude d'algorithmes performants de résolution du logarithme discret. La cryptographie étudie les moyens sécurisés de transmettre des informations, de les chiffrer et de les déchiffrer par des algorithmes dits cryptosystèmes. La majorité des cryptosystèmes actuels repose sur la difficulté de factoriser des grands entiers ou de calculer des logarithmes discrets dans un groupe fini. La résolution du logarithme discret consiste à déterminer les exposants d'une famille fixée de générateurs dans la décomposition des éléments du groupe. Dans le cas des groupes multiplicatifs d'un corps fini, la complexité des calculs dépendent de la taille - dite de petite, moyenne ou grande caractéristique- de la caractéristique du corps dans lesquels on effectue les calculs.
Nous présentons différents algorithmes dans chacune des caractéristiques (petite, moyenne ou grande) en précisant quel est l'algorithme le plus performant dans chacun des cas. Nous nous intéressons particulièrement à la détermination de classes de polynômes à coefficients petits par rapport à la taille du corps. Ces polynômes définissent des extensions de corps sur lesquelles les calculs de déchiffrement deviennent les plus efficaces.

La seconde partie s'inscrit dans le contexte du programme de Langlands p-adique. Même si la correspondance de Langlands p-adique est connue en dimension deux pour $\mathbb{Q}_p$ depuis environ cinq ans avec les travaux de Breuil, Colmez, Emerton et Kisin, le cas de la dimension supérieure reste à ce jour ouvert.
Nous présentons une généralisation de l'un des outils centraux de la théorie, les modules de Breuil-Kisin, en dimension supérieure. Nous définissons une version multi-variée des modules de Breuil-Kisin où la tour de Lubin-Tate remplace la tour cyclotomique classique. Il s'agit ensuite de revisiter la preuve de Kisin du plongement pleinement fidèle de la catégorie des représentations cristallines dans la catégorie des modules de Breuil-Kisin. Malheureusement certains arguments classiques ne se généralisent pas au cas de dimension supérieure. Il convient alors de développer de nouvelles stratégies, plus proches des résultats en équi-caractéristique de Genestier et Lafforgue.

La troisième partie est un travail effectué en collaboration avec Victor Vilaça Da Rocha, Roberta Tittarelli, Richard Sambilason Rafefimanana, Victor Michel-Dansac et Benjamin Couéraud. Il a été initié lors de la treizième SEME, Semaine d'Etudes Maths Entreprises organisée par l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société (AMIES).
L'Institut Français du Pétrole et des Energies Nouvelles nous a soumis un problème de résolution numérique d'un système d'équations modélisant la

désorption d'un gaz de schiste en une dimension. Nous proposons plusieurs schémas du premier ordre recourant à un traitement implicite de l'équation de relaxation. Enfin nous présentons un schéma numérique d'ordre deux en temps.

En annexe est reporté un article de diffusion paru dans la rubrique "l'objet du mois" du site Image des Maths, rubrique consacrée à la présentation d'objets mathématiques. Il s'agit d'une transcription pour Images des Maths d'un travail de Mark Baker, Jane Beltran, Jason Buell, Brian Conrey, Tom Davis, Brianna Donaldson, Jeanne Detorre-Ozeki, Leila Dibble, Tom Freeman, Robert Hammie, Julie Montgomery, Avery Pickford et Justine Wong effectué et publié dans le cadre du "Math Teacher's Circle".
Le jeu Set est l'illustration, probablement la plus connue, de la géométrie d'un espace vectoriel de dimension 4 sur $\mathbf{F}_3$. Les règles du jeu utilisent les droites, les plans et les hyperplans de cet espace qu'il s'agit d'identifier le plus rapidement possible. Une étude combinatoire révèle les chances d'apparition -et l'intérêt du jeu !- de tels objets géométriques après le tirage aléatoire d'un nombre fixé de points de l'espace.

Part I

Logarithme discret en cryptographie

1 Introduction

Le logarithme discret est apparu en cryptographie dans l'article de Diffie et Hellmann en 1976 ([DH]) pour le cryptage par clé publique entre deux utilisateurs Alice et Bob. On fixe un groupe fini, cyclique G et un générateur g de G qui est connu d'Alice et Bob. Il est commode de prendre pour G, le groupe des éléments inversibles d'un corps fini. Alice (respectivement Bob), choisit (de façon secrète) un entier "assez grand" a (respectivement b). Alice (respectivement Bob) élève g à la puissance a (respectivement b). Les éléments g^a et g^b de G sont rendus publiques. De ce fait, Alice dispose de la connaissance de g^b et de a. Ainsi Alice et Bob connaissent tous deux g^{ab} sans l'avoir transmis.
Diffie et Hellmann ([DH]) conjecturent que le problème consistant à casser ce protocole est aussi difficile que le problème de résolution du logarithme discret, autrement dit, connaissant $g \in G$ et g^a, trouver a.
L'objet de notre travail est présenter quelques aspects de la résolution du logarithme discret dans G groupe multiplicatif d'un corps fini. Nous nous intéressons particulièrement à la complexité des algorithmes mis en œuvre. La méthode du calcul d'indice initiée par Kraitchik en 1922 ([Kr]) a été adaptée à la cryptographie par Diffie et Hellmann ([DH]) et Adleman ([Ad1]).
Plus récemment, de nouveaux algorithmes efficaces sont apparus via le crible par corps de fonctions, en petite caractéristique ([Ad2] et [JL]) ou le crible par corps de nombres en moyenne et grande caractéristiques ([JL], [JLSV] et [BGGM]). Tous ces algorithmes sont de complexité sous-exponentielle.

Ce chapitre est organisé comme suit. Dans la section §2, on présente la méthode du calcul d'indice pour la détermination du logarithme discret sur le groupe multiplicatif du corps fini $\mathbb{F}_{p^n}$. L'efficacité de cette méthode dépend de la borne de lissité choisie sur la famille de générateurs de $\mathbb{F}_{p^n}^*$.

Dans la section §3, le théorème de Canfield-Erdos-Pomerance (§3.1) fournit une majoration de la complexité des algorithmes associés à la méthode du calcul d'indice. La méthode de détermination du logarithme discret dépend de la "taille" (petite, moyenne ou grande) de la caractéristique du corps fini sur lequel on travaille (§3.4). Les sections suivantes précisent ces calculs de complexité pour les algorithmes les plus efficaces dans chacun des cas : petite caractéristique (§4), grande et moyenne (§8, §9).

Dans la section §4, on présente brièvement le crible par corps de fonctions, crible optimal en petite caractéristique d'après [BGJT]. Il repose sur la présentation du corps fini comme un anneau quotient d'un anneau de polynômes.

Dans la suite de ce texte, on s'intéresse uniquement au cas de la grande ou

moyenne caractéristique. D'abord (§5), on détaille la méthode du crible par corps de nombres. Celle-ci repose sur une présentation du corps fini comme quotient d'anneaux d'entiers de corps de nombres. Via le choix de deux présentations (identiques ou différentes en utilisant deux anneaux d'entiers distincts), on construit une famille de relations linéaires entre éléments d'une famille génératrice de $\mathbb{F}_{p^n}^*$ (§5.1). La résolution de ce système linéaire détermine le logarithme discret.
Les anneaux d'entiers de corps de nombres étant de Dedekind, chaque idéal se décompose en produits d'idéaux premiers. Malheureusement, cette décomposition n'est unique qu'à choix fixé d'une famille génératrice des unités et de générateurs de chaque idéal premier.
L'application de Shirokauer (§5.2) permet d'associer à chaque idéal de façon unique des puissances de générateurs fixés d'idéaux premiers. Les exposants introduits par l'application de Shirokauer admettent une interprétation arithmétique en termes de nombres de classes de certains anneaux d'entiers.
Il s'agit enfin de déduire de ces constructions le crible par corps de nombres, c'est-à-dire, d'expliciter comment obtenir le logarithme discret à partir des informations ainsi obtenues (§5.3).

La section §6 est consacrée à la construction des corps de nombres qui apparaissent lors de l'usage de la méthode du crible. On commence par un court paragraphe de rappels sur la notion de résultant (§6.1). Les propriétés recherchées sur les différents polynômes définissant les corps de nombres utilisés par le crible, s'interprètent, en effet, de façon explicite et calculatoire en termes de résultants. On rappelle ensuite (§6.2) la construction initiale de Joux-Lercier (§[JLSV]).
Dans (§6.3), on propose une construction alternative de ces polynomes qui déterminent un nouvel algorithme pour le calcul du logarithme discret et on calcule sa complexité.

Dans la section §7, on propose une autre stratégie de construction des extensions finies de $\mathbb{Q}$ utilisées dans le crible par corps de nombres. D'après §6.1, on sait caractériser les polynômes optimaux recherchés, i.e. dont les racines sur $\mathbb{C}$ engendrent les "meilleurs" corps de nombres pour le crible. La construction de §7 repose sur le choix d'un élément de $\mathbb{F}_p$ dont les puissances restent "petites". Malheureusement, il s'avère que de tels éléments sont très rares : la probabilité d'obtenir un tel élément est de l'ordre de $1/p^{2n}$ ce qui rend la méthode de la section §7 inutilisable en pratique.

La section §8 est dédiée aux calculs de complexité des différents algorithmes avec corps de nombres (§6.3) entre moyenne et grande caractéristique.

Une discontinuité de la valeur de la complexité apparaît entre les cas de petite et moyenne caractéristiques (§9). Cette observation justifie le raffine-

ment dans le calcul de complexité en moyenne caractéristique. D'abord on constate qu'au voisinage de la petite caractéristique, on ne peut plus négliger l'influence du calcul du résultant dans la complexité en moyenne caractéristique (§9.1).
Dans §9.2, la minoration des différents coefficients du résultant suggère qu'il y a explosion de la complexité de la méthode du crible par corps de nombres quand on approche du cas limite de la petite caractéristique. Ce dernier point suggère la vanité de notre approche au voisinage de la petite caractéristique.

Enfin on présente dans la dernière partie (§10), les avancées les plus récentes sur la détermination du logarithme discret. Il s'agit d'une part du crible multiple par corps de nombres (§10.1) dû à Barbulescu et Pierrot ([BP]) et d'autre part du crible par tour de corps de nombres (§10.2) dû à Barbulescu et Kim ([BK]). Nous présentons les grandes lignes de leurs méthodes et quelques pistes nouvelles pouvant induire des variantes possibles.

Ce travail n'aurait jamais vu le jour sans la bienveillance d'Antoine Joux et de Cécile Pierrot qui n'ont ménagé ni leur temps ni leur patience pour m'expliquer les différents aspects de leurs algorithmes. Je dois notamment à Cécile cette discussion fine sur les différents algorithmes pertinents en fonction de la caractéristique, la construction des polynômes utiles et l'étude des cas limites entre petite et moyenne caractéristique.

2 Méthode du calcul d'indice

On fixe un nombre premier p, un entier $n \geq 1$ et un générateur g de $\mathbb{F}_{p^n}^*$.

Définition 2.1. *On appelle logarithme discret de $x \in \mathbb{F}_{p^n}^*$ le plus petit entier positif h tel que $x = g^h$.*

Pour calculer les logarithmes discrets des éléments de $\mathbb{F}_{p^n}^*$, on les décompose dans une famille génératrice privilégiée.

Le temps de calcul de cette décomposition doit être aussi petit que possible. Cela impose des conditions sur le choix de la famille génératrice ou, plus précisément, sur un choix d'éléments relevant cette famille dans un anneau dans lequel il est pratique de faire les calculs. On identifie alors $\mathbb{F}_{p^n}$ au quotient de cet anneau par un idéal maximal approprié.
Il est plus facile de décomposer un nombre entier en produit de nombres premiers si l'on possède une borne (la plus petite possible) majorant la taille de ses facteurs premiers. L'analogue existe pour les anneaux d'entiers ou les anneaux de polynômes. Ainsi on définit la notion de borne de lissité :

Définition 2.2. *Soit B un entier naturel fixé.*
(i) Soit $x \in \mathbb{Z}$, on dit que x est B-lisse lorsque tous les diviseurs premiers de

x sont plus petits que B.
(ii) Soit $x \in \mathbb{Z}[X]$, on dit que x est B-lisse lorsque tous les diviseurs premiers de x sont de degrés plus petits que B.
(iii) Soit x un idéal premier d'un anneau d'entiers $\mathcal{O}$, on dit que x est B-lisse si la norme de x (le cardinal du corps fini $\mathcal{O}/x$) est B-lisse au sens de (i).

La définition 2.2 est importante pour la suite. En effet, supposons donnée une famille $\{g_i\}_{i\in I}$ d'éléments de $\mathbb{F}_{p^n}^*$ générant ce groupe cyclique. Supposons, de plus que pour tout i dans I, il existe un relèvement de g_i dans $\mathbb{N}$ qui soit B-lisse (au sens de (i) 2.2). Alors ([LO]) il existe un algorithme de complexité quasi-polynomiale en le logarithme de B décomposant tout élément du groupe cyclique $\mathbb{F}_{p^n}^*$ dans la base $\{g_i\}_{i\in I}$. De tels algorithmes existent aussi pour des relèvements dans des anneaux de polynômes ou des anneaux d'entiers ([LO]).
Calculer le logarithme discret d'un élément quelconque de $\mathbb{F}_{p^n}^*$ se ramène donc, après décomposition dans la famille des $\{g_i\}_{i\in I}$, au seul calcul du logarithme discret des g_i.
Le calcul d'indice est une méthode résolvant le problème du logarithme discret. Il consiste à recueillir suffisamment de relations sur les $\{g_i\}_{i\in I}$ pour en déduire leur logarithme. Ces relations sont de la forme

$$\prod_{i\in I} g_i^{h_i} = \prod_{i\in I} g_i^{h'_i}$$

où les h_i et h'_i sont des éléments de $\mathbb{Z}$. En passant au logarithme discret (noté log) on obtient :

$$\sum_{i\in I} h_i \log(g_i) \equiv \sum_{i\in I} h'_i \log(g_i) \mod p^n - 1. \tag{2.1}$$

Si on obtient assez de relations de type (2.1), on peut en déduire un système d'équations linéaires d'inconnues $\log(g_i)$ pour tout i dans I. Un tel système, s'il est inversible, permet d'obtenir pour tout i dans I les valeurs $\log(g_i)$.
Pour déterminer le logarithme discret d'un élément quelconque x de $\mathbb{F}_{p^n}^*$, il suffit alors de le décomposer dans la famille $\{g_i\}_{i\in I}$:

$$x = \prod_{i\in I} g_i^{h_i}.$$

Ainsi $\log(x) = \sum_{i\in I} x_i \log(g_i)$. On obtient de la sorte un algorithme résolvant le problème du logarithme discret dans $\mathbb{F}_{p^n}^*$.

3 Familles génératrices d'éléments lisses

La méthode du calcul d'indice s'effectue donc en deux phases, la phase de détermination de la famille génératrice satisfaisant l'hypothèse de lissité, puis la phase de collection d'un nombre suffisant de relations pour calculer

les logarithmes discrets.
Pour majorer la complexité de la première phase, la détermination d'une famille génératrice, on s'appuie sur le théorème suivant dû à Canfield-Erdos-Pomerance, ([CEP]).

Théorème 3.1. *Soit A et B deux entiers naturels, $B > 2$. La densité des nombres entiers positifs inférieurs ou égaux à A B-lisses est donnée par $u^{-u+o(1)}$ où $u = \ln(A)/\ln(B)$ et $o(1)$ tend vers 0 quand A tend vers l'infini.*

Le théorème 3.1 fournit donc une borne supérieure à la probabilité d'obtenir un élément B-lisse inférieur à A. Remarquons que ce théorème admet une version polynomiale :

Théorème 3.2. *Soit A et B deux entiers naturels. La densité qu'un polynôme de $\mathbb{Z}[X]$ de degré inférieur ou égal à A soit B-lisse est donnée par $u^{-u+o(1)}$ où $u = \ln(A)/\ln(B)$ et $o(1)$ tend vers 0 quand A tend vers l'infini.*

La complexité d'un algorithme s'identifie à sa partie la plus coûteuse. On peut donc supposer la complexité de ces deux phases (détermination, collection) égales. La première consiste en la recherche d'éléments B-lisses via le théorème de Canfield-Erdos-Pomerance. La seconde, d'algèbre linéaire, consiste en la résolution du système donné par les équations de la forme (2.1). Soit v le logarithme (népérien) d'une borne sur la taille des éléments lisses : cette borne est notée A dans le théorème 3.1. Alors, d'après le théorème 3.1, il existe λ et μ deux réels, que l'on calcule explicitement dans la section §8, tels que la complexité de l'algorithme global, identifié à sa partie de collecte d'éléments B-lisses, soit de la forme :

$$(\lambda v)^{\mu v + o(1)}.$$

On identifie les éléments candidats à la B-lissité à des relèvements d'éléments de $\mathbb{F}_{p^n}$, on peut donc les choisir inférieurs ou égaux à p^n si l'anneau du relèvement s'identifie à $\mathbb{Z}$.
Dans le cas où le relèvement s'effectue dans un anneau d'entiers, on demande (voir 5.1) à ce que les éléments lisses engendrent à des idéaux maximaux de cet anneau d'entiers. On ne cherche alors d'éléments lisses que parmi les idéaux dont la norme est inférieure ou égale à p^n.

Ainsi on peut poser en suivant les notations du théorème 3.1 $A = p^n$. En d'autres termes, on peut supposer $v = \ln(p^n)$. On introduit alors la notation suivante :

Définition 3.3. *On pose $q = p^n$ et*

$$L_q(a, c) = \exp\left((c + o(1))(\ln(q)^a(\ln(\ln(q)))^{1-a})\right)$$

avec $0 \leq a \leq 1$ et c de l'ordre de 1.

La fonction $L_q(a,c)$ introduite dans la définition 3.3 est un moyen utile pour paramétrer différents objets qui interviennent dans le calcul de complexité de l'algorithme d'indice.
D'abord la complexité globale de l'algorithme de calcul d'indice s'exprime sous la forme d'une fonction $L_q(a,c)$ (voir §8). Les constantes a et c de la définition 3.3 se déduisent aisément de λ et μ si l'on pose $v = \ln(q)$. En particulier, si $a = 0$, la complexité est polynomiale en $\ln(q)$. Si $a = 1$ la complexité est exponentielle en $\ln(q)$. La complexité est minimale si a et c sont minimaux.
Ensuite la fonction $L_q(a,c)$ permet de classer les nombres premiers p étudiés. Précisément si l'on écrit p sous la forme :

$$p = L_q(l,c),$$

on a la définition suivante :

Définition 3.4. *Soit p un nombre premier, n un entier naturel et $q = p^n$. On pose $p = L_q(l,d)$ avec $0 \leq l \leq 1$ et d de l'ordre de 1.*
Si $l < 1/3$, l'extension $\mathbb{F}_{p^n}$ est dite de petite caractéristique.
Si $1/3 \leq l \leq 2/3$ elle est dite de moyenne caractéristique.
Sinon, $\mathbb{F}_{p^n}$ est dite de grande caractéristique.

Par exemple, si p est quelconque et $n = \lfloor p/\ln(p) \rfloor$ l'extension est de petite caractéristique. Pour p quelconque et $n = 1$, l'extension est de grande caractéristique. Cette distinction a son importance pour deux raisons :
- la première, c'est que suivant que p est de petite, moyenne ou grande caractéristique, ce sont des algorithmes différents qui donnent les meilleurs résultats en termes de complexité. L'anneau quotienté pour présenter $\mathbb{F}_{p^n}$, le choix de la base de lissité et la collecte de relation sur cette base sont différents.
- La seconde raison est que, dans les calculs de complexité, les termes négligeables ne sont pas les mêmes- suivant la caractéristique -petite, moyenne ou grande- de $\mathbb{F}_{p^n}$ (voir section §8).

La partie §4 traite succinctement des méthodes utilisées en petite caractéristique. Les anneaux quotientés utilisés pour présenter $\mathbb{F}_{p^n}$ sont alors des anneaux de polynômes sur $\mathbb{F}_p$. On ne détaille pas le calcul de la complexité en petite caractéristique. En effet, à partir de la section §5, on se limite à l'étude de la moyenne et grande caractéristique.

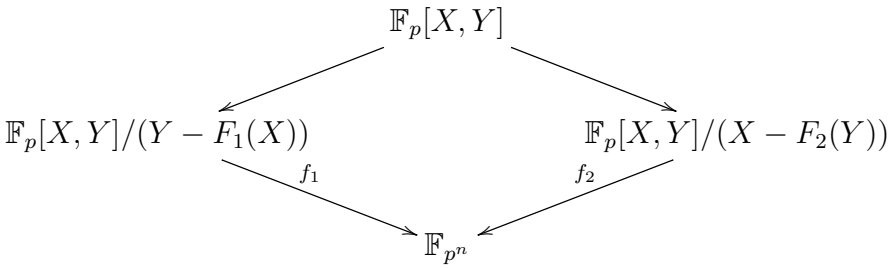
4 Petite caractéristique

En petite caractéristique (voir [BGJT]) on identifie $\mathbb{F}_{p^n}$ à un quotient par un idéal maximal de $\mathbb{F}_p[X,Y]$ où $\mathbb{F}_p[X,Y]$ représente l'anneau des polynômes en deux variables sur $\mathbb{F}_p$.

Soient F_1 et F_2 deux polynômes sur $\mathbb{F}_p$ en une variable tels que $F_2(F_1(X))-X$ est divisible par un polynôme irréductible noté Φ de degré n sur $\mathbb{F}_p$. Soit θ une racine de Φ. Ainsi θ engendre $\mathbb{F}_{p^n}$. En envoyant X sur $F_2(\theta)$ (respectivement Y sur $F_1(\theta)$), on peut définir les morphismes d'anneaux

$$f_1 : \mathbb{F}_p[X,Y]/(Y - F_1(X)) \to \mathbb{F}_{p^n} \text{ et } f_2 : \mathbb{F}_p[X,Y]/(X - F_2(Y)) \to \mathbb{F}_{p^n}.$$

Le diagramme suivant est alors commutatif



La base choisie de lissité est la projection par f_1 (respectivement f_2) de famille de polynômes B-lisses dans $\mathbb{F}_p[X,Y]/(Y - F_1(X))$ (respectivement $\mathbb{F}_p[X,Y]/(X - F_2(Y))$). On souhaite, dans cette partie §4, mettre l'accent sur le fait que la collecte de relations, le choix de la base de lissité et la présentation du groupe étudié, s'appuie sur des anneaux de polynômes sur $\mathbb{F}_p$ en petite caractéristique. Pour une analyse détaillée du choix de F_1 et F_2 ainsi que de la base de lissité on renvoie encore à [BGJT]. On ne détaille pas cette construction mais il est plus facile de factoriser dans des anneaux de polynômes sur $\mathbb{F}_p$ que dans des anneaux d'entiers.
Les algorithmes les plus récents sont même de complexité polynomiale (voir [Jo]). Ainsi le coût du calcul du logarithme individuel d'un élément quelconque de $\mathbb{F}_{p^n}^*$ est essentiellement dû au calcul de sa décomposition dans la base de lissité. On obtient actuellement une complexité de l'ordre de $\mathrm{L}_{p^n}(a,c')$ si p est de la forme $\mathrm{L}_{p^n}(a,c)$. On parle alors de complexité quasi-polynomiale ([BGJT]).

5 Moyenne et grande caractéristique

Dans cette partie, on détaille la méthode de crible par corps de nombres qui donne, pour la moyenne et la grande caractéristique, de meilleurs résultats que le crible par corps de fonctions évoqué dans la partie précédente (§4). Dans §5.1, on donne un aperçu général de cette méthode. D'abord on définit un modèle du logarithme discret dans les anneaux d'entiers, dit logarithme virtuel (§5.2). Puis on retrouve (§5.3) le logarithme discret pour tout élément de $\mathbb{F}_{p^n}^*$. La construction des corps de nombres est détaillée dans la section §6.

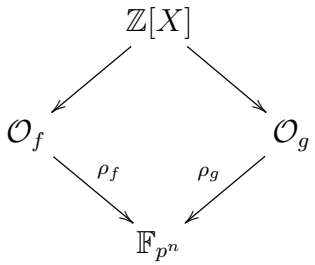
5.1 Méthode du crible par corps de nombres

Dans la méthode du crible par corps de nombres, on remplace les corps de fonctions de la section §4 par des corps de nombres. La base de lissité se déduit alors des idéaux premiers de leurs anneaux d'entiers. Nous détaillons ici la construction commune à toutes les méthodes dites de crible par corps de nombres de [BGGM].

On commence par construire deux polynômes f et g de $\mathbb{Z}[X]$ irréductibles unitaires et possédant une racine commune modulo p engendrant $\mathbb{F}_{p^n}$. On note m la racine commune de f et g modulo p identifiant $\mathbb{F}_p[m]$ à $\mathbb{F}_{p^n}$. Soit α et β des racines dans $\mathbb{C}$ de respectivement f et g. On note

$$K_f = \mathbb{Q}[\alpha] \text{ et } K_g = \mathbb{Q}[\beta].$$

Pour K_f (respectivement K_g) on note $\mathcal{O}_f$ (respectivement $\mathcal{O}_g$) l'anneau d'entiers associé. On rappelle que l'anneau d'entiers d'un corps de nombres est l'ensemble des éléments de ce corps racines d'un polynôme unitaire de $\mathbb{Z}[X]$. On peut alors définir le diagramme suivant :



En d'autres termes, le corps $\mathbb{F}_{p^n}$ s'obtient ici comme la réduction modulo un idéal premier au dessus de p de $\mathcal{O}_f$ et de $\mathcal{O}_g$.

On rappelle la définition suivante :

Définition 5.1. *Soit A un anneau commutatif intègre. Soient I et J deux idéaux de A. On dit que I est équivalent à J, s'il existe a et b dans A tels que $aI = bJ$. Le nombre de classes de A est le cardinal du quotient de l'ensemble des idéaux de A par cette relation d'équivalence.*

Notons h le nombre de classes de $\mathcal{O}_f$ (on dit aussi nombre de classes de K_f). Pour tout $\mathfrak{p}$ idéal premier de $\mathcal{O}_f$ l'idéal $\mathfrak{p}^h$ est alors principal mais le choix d'un générateur de cet idéal n'est connu qu'à unité près.
Notons r l'entier tel que $r = r_1 + r_2 - 1$ où r_1 est le nombre de racines réelles de f et r_2 le nombre de racines dans $\mathbb{C}$ qui ne sont pas réelles.
Soit U_f le groupe des unités de $\mathcal{O}_f$. D'après le théorème de Dirichlet, on a :

$$U_f \simeq U_{tor} \times \mathbb{Z}^r$$

où U_{tor} est cyclique : c'est la partie de U_f formée des racines de l'unité de $\mathbb{C}$ incluses dans K_f. Fixons ε_0 un générateur de U_{tor} et une famille génératrice $\{\varepsilon_i\}_{i\in\{1,\dots,r\}}$ de la partie sans torsion de U_f.
Fixons une borne de lissité B (elle n'est explicitée que lors du calcul de complexité de la section §8). On note $\mathcal{F}_f$ l'ensemble des idéaux premiers $\mathfrak{p}$ de $\mathcal{O}_f$ dont les normes, c'est-à-dire le cardinal de $\mathcal{O}_f/\mathfrak{p}$, sont plus petites que B.
Soit $\mathfrak{q}$ un élément de $\mathcal{F}_f$ et $b_\mathfrak{q}$ le choix d'une bijection du groupe engendré par les $\{\varepsilon_i\}_{i\in\{0,\dots,r\}}$ avec l'ensemble des générateurs de $\mathfrak{q}^h$. On note Γ l'ensemble :

$$\Gamma = \{\varepsilon_i\}_{i\in\{0,\dots,r\}} \cup \{b_\mathfrak{q}\}_{\mathfrak{q}\in\mathcal{F}_f}.$$

La donnée de Γ permet d'associer à $\mathfrak{q}^h$ un de ses générateurs que l'on note $\gamma_\mathfrak{q}$. D'après la définition 2.1, un logarithme discret est déterminé par la donnée d'un générateur du groupe étudié. L'algorithme d'Hellman Pohlig ([HP]) permet de décomposer en parties élémentaires le problème du logarithme discret. Précisément, pour tout l diviseur premier de p^n-1, l'algorithme calcule le logarithme discret dans $\mathbb{F}_{p^n}^* \simeq \mathbb{Z}/(p^n-1)\mathbb{Z}$ pourvu qu'on connaisse l'ordre de cet élément réduit modulo l, c'est-à-dire dans $\mathbb{Z}/l\mathbb{Z}$. On travaille à présent à l fixé. On choisit $\mathcal{F}_f$ comme base de lissité dans $\mathcal{O}_f$. Soit $\mathfrak{q}$ dans $\mathcal{F}_f$, on définit le logarithme virtuel de $\mathfrak{q}$ de la manière suivante :

Définition 5.2. *Soit $\mathfrak{q} \in \mathcal{F}_f$ et $\gamma_\mathfrak{q}$ le générateur de $\mathfrak{q}^h$ associé à Γ. Le logarithme discret virtuel de $\mathfrak{q}$ modulo l est :*

$$\log_\Gamma(\mathfrak{q}) = h^{-1}\log(\rho_f(\gamma_\mathfrak{q})) \mod l.$$

De même, pour une unité fondamentale ε_i on pose :

$$\log_\Gamma(\varepsilon_i) = h^{-1}\log(\rho_f(\varepsilon_i)) \mod l, 0 \leq i \leq r.$$

Remarque 5.3. *Les éléments $\log_\Gamma(\mathfrak{q})$ et $\log_\Gamma(\varepsilon_i)$ de $\mathbb{Z}/l\mathbb{Z}$ sont appelés communément des logarithmes virtuels car ces derniers représentent virtuellement, c'est-à-dire relevés aux anneaux d'entiers, les logarithmes discrets dans $\mathbb{F}_{p^n}^*$.*

Si φ est un polynôme de $\mathbb{Z}[X]$ de degré inférieur ou égal à $t-1$ (l'entier t est ensuite fixé) et α une racine fixée de f dans $\mathbb{C}$. On dit que $\varphi(\alpha)$ est B-lisse si l'idéal principal $\varphi(\alpha)\mathcal{O}_f$ se décompose en idéaux premiers B-lisses. Dans les calculs de complexité de la section §8, on fixe t et on optimise B. Par suite, on peut supposer que $\mathcal{F}_f$ est formé d'idéaux engendrés par des polynômes de degrés tous inférieurs à $t-1$. Pour $\varphi(\alpha)$ élément B-lisse, l'idéal $\varphi(\alpha)\mathcal{O}_f$ se décompose en idéaux premiers tous éléments de $\mathcal{F}_f$:

$$\varphi(\alpha)\mathcal{O}_f = \prod_{\mathfrak{q}\in\mathcal{F}_f} \mathfrak{q}^{\mathrm{val}_\mathfrak{q}(\varphi(\alpha))} \tag{5.1}$$

où $\mathrm{val}_\mathfrak{q}(\varphi(\alpha))$ désigne la multiplicité de $\mathfrak{q}$ dans la décomposition de $\varphi(\alpha)$.
Ainsi, en élevant l'identité (5.1) à la puissance h, il existe une unique famille

d'entiers $\{e_{i,\varphi(\alpha)}\}_{i\in\{0,\dots,r\}}$ tels que :

$$\varphi(\alpha)^h = \varepsilon_0^{e_{0,\varphi(\alpha)}} \prod_{i=1}^{r} \varepsilon_i^{e_{i,\varphi(\alpha)}} \prod_{\mathfrak{q}\in\mathcal{F}_f} \gamma_{\mathfrak{q}}^{\mathrm{val}_{\mathfrak{q}}(\varphi(\alpha))}.$$

On peut appliquer le morphisme d'anneaux $\rho_f : \mathcal{O}_f \to \mathbb{F}_{p^n}$ et on obtient après passage au logarithme discret dans $\mathbb{F}_{p^n}^*$:

$$\log(\rho_f(\varphi(\alpha))) = e_{0,\varphi(\alpha)}\log_\Gamma(\epsilon_0) + \sum_{i=1}^{r} e_{i,\varphi(\alpha)}\log_\Gamma(\varepsilon_i) + \sum_{\mathfrak{q}\in\mathcal{F}_f} \mathrm{val}_{\mathfrak{q}}(\varphi(\alpha))\log_\Gamma(\mathfrak{q}).$$

On peut raisonner de même dans $\mathcal{O}_g$ pour β une racine fixée de g dans $\mathbb{C}$ et l'on trouve :

$$\log(\rho_f(\varphi(\alpha))) = \log(\rho_g(\varphi(\beta))).$$

On en déduit, en faisant varier $\varphi \in \mathbb{Z}[X]$, des relations linéaires, en nombre égal aux nombres de $\varphi(\alpha)\mathcal{O}_f$ décomposés. Ces relations portent sur les éléments de la forme $\log_{\Gamma_f}(\epsilon_{i,f})$, $\log_{\Gamma_g}(\epsilon_{i,g})$ et $\log_{\Gamma_f}(\mathfrak{q}_\mathfrak{f})$, $\log_{\Gamma_g}(\mathfrak{q}_\mathfrak{g})$ où l'on a mis f et g en indice pour distinguer les contributions des deux corps, K_f et K_g considérés. Ainsi, en décomposant suffisamment d'éléments de la forme $\varphi(\alpha)\mathcal{O}_f$ et $\varphi(\beta)\mathcal{O}_g$, précisément au moins

$$r_f + r_g + 2 + \#(\mathcal{F}_f) + \#(\mathcal{F}_g),$$

tels éléments, on peut résoudre le système et obtenir $\log_{\Gamma_f}(\mathfrak{q}_\mathfrak{f})$ (et $\log_{\Gamma_g}(\mathfrak{q}_\mathfrak{g})$) pour tout $\mathfrak{q}_f$ (et $\mathfrak{q}_g$) dans $\mathcal{F}_f$ (et $\mathcal{F}_g$).

Remarque 5.4. *Dans le calcul du logarithme, on a généralement* $\log_\Gamma(\varepsilon_0) = 0 \mod l$. *En effet, si* ε_0 *est une racine de l'unité d'ordre* r_0 *tel que* hr_0 *soit premier avec* l, *on a* $\varepsilon_0^{r_0} = 1$ *et par suite* $hr_0\log_\Gamma(\varepsilon_0) = 0 \mod l$, *donc* $\log_\Gamma(\varepsilon_0) = 0 \mod l$.

Cette approche a quelques limites liées à la détermination des données nécessaires à l'algorithme mis en œuvre :
- le nombre de classes h de K_f,
- le choix des générateurs de U_f,
- le choix d'un générateur de $\mathfrak{q}^h$ pour tout $\mathfrak{q}$ élément de $\mathcal{F}_f$.

En général, pour un polynôme f dont les coefficients sont de l'ordre de $p^{1/2}$, ces données ne sont pas accessibles rapidement.
Cette remarque justifie l'introduction d'une autre définition, indépendantes des unités, des logarithmes discrets des éléments de $\mathcal{F}_f$ (voir Définition 5.6).

5.2 Applications de Schirokauer

On garde les notations définies dans la partie §5.1, notamment K_f est un corps de rupture du polynôme $f \in \mathbb{Z}[X]$. On introduit la notion suivante :

Définition 5.5. *Soit l et r deux entiers et K_f un corps de rupture de $f \in \mathbb{Z}[X]$. On définit K_l comme l'ensemble des éléments de K_f^* de normes premières à l. Une application de Schirokauer Λ est une surjection linéaire*

$$\Lambda : (K_l)/(K_l)^l \to (\mathbb{Z}/l\mathbb{Z})^r,$$

$$\forall(\gamma_1, \gamma_2) \in \left((K_l)/(K_l)^l\right)^2 : \ \Lambda(\gamma_1\gamma_2) = \Lambda(\gamma_1) + \Lambda(\gamma_2),$$

et Λ est surjective des unités de K_f sur $(\mathbb{Z}/l\mathbb{Z})^r$:

$$\Lambda(U_f) = (\mathbb{Z}/l\mathbb{Z})^r.$$

Dans [Sc2], Schirokauer construit une telle application. On reprend ici sa construction.
Soit Δ l'ensemble des degrés des facteurs irréductibles de $f \mod l$. On pose e dans $\mathbb{N}$ le plus petit commun multiple des éléments de la forme $l^\delta - 1$, pour $\delta \in \Delta$. Ainsi d'après le petit théorème de Fermat, pour tout $\gamma(X)$ dans $\mathbb{Z}[X]$ tel que $\gamma(\alpha)$ appartient à K_l on a :

$$\gamma(X)^e - 1 \mod (f(X), l) = 0.$$

Par suite on peut bien définir une application

$$\Lambda_0 : (K_l)/(K_l)^l \longrightarrow \mathbb{Z}/l\mathbb{Z}[X]/(f(X))$$

par :

$$\gamma(\alpha) \mapsto \frac{\gamma(X)^e - 1}{l} \mod (f(X), l).$$

En pratique ([Sc2]), si $1, X, \ldots, X^{r-1}$, sont les r premiers termes de la famille génératrice $1, X, \ldots, X^{\deg(f)-1}$ de $\mathbb{Z}/l\mathbb{Z}[X]/(f(X))$ la projection de Λ_0 sur l'espace engendré par ces r premiers termes est une application de Schirokauer que l'on note Λ.
Comme $\Lambda(U_f) = (\mathbb{Z}/l\mathbb{Z})^r$, il existe une famille $(\varepsilon_i)_{1\leq i\leq r}$ génératrice de U_f telle que $\Lambda(\varepsilon_i) = (0, \ldots, 0, h, 0, \ldots, 0)$ où la composante égale à h est à la i-ème position. C'est cette famille qui va permettre de définir le logarithme virtuel associé à Λ.
Remarquons que $\Lambda(U_f) = (\mathbb{Z}/l\mathbb{Z})^r$ permet aussi d'assurer l'existence de $\gamma_\mathfrak{q}$ générateur de $\mathfrak{q}^h$ tel qu'on ait : $\Lambda(\gamma_\mathfrak{q}) = 0$. En effet, U_f agit transitivement sur les générateurs de $\mathfrak{q}^h$. Ainsi, pour un générateur arbitraire donné q de $\mathfrak{q}^h$,on peut construire un nouveau générateur $\gamma_\mathfrak{q}$ de $\mathfrak{q}^h$ tel que $\Lambda(\gamma_\mathfrak{q}) = 0$. De plus, $\gamma_\mathfrak{q}$ est défini à racine de l'unité près. La remarque 5.4 permet alors de définir le logarithme discret associé à Λ :

Définition 5.6. *Soit Λ une application de Schirokauer, $\mathcal{F}_f$ l'ensemble des idéaux premiers de $\mathcal{O}_f$, B-lisse pour un certain réel B, $\mathfrak{q}$ un idéal de $\mathcal{F}_f$ et $\gamma_\mathfrak{q}$ un générateur de la puissance h-ième de $\mathfrak{q}$ vérifiant $\Lambda(\gamma_\mathfrak{q}) = 0$. Le logarithme virtuel associé à Λ de l'idéal $\mathfrak{q}$ est défini par :*

$$\log_\Lambda(\mathfrak{q}) = h^{-1}\log(\rho_f(\gamma_\mathfrak{q})) \mod l.$$

De même, le logarithme virtuel associé à Λ d'une unité fondamentale est défini par l'expression :

$$\log_\Lambda(\varepsilon_i) = h^{-1}\log(\rho_f(\varepsilon_i)) \mod l, \quad 0 \leq i \leq r.$$

On peut raisonner comme dans 5.1 : si α est une racine complexe de f et si φ est un polynôme de $\mathbb{Z}[X]$, on obtient en décomposant l'idéal $\varphi(\alpha)\mathcal{O}_f$ selon les idéaux premiers de $\mathcal{F}_f$ la relation suivante :

$$\log(\rho_f(\varphi(\alpha))) = \sum_{i=1}^{r} \lambda_i(\varphi(\alpha))\log_\Lambda(\epsilon_i) + \sum_{\mathfrak{q}\in\mathcal{F}_f} \mathrm{val}_\mathfrak{q}(\varphi(\alpha))\log_\Lambda(\mathfrak{q}) \mod l$$

où les $(\lambda_i)_{1\leq i\leq r}$ sont les composantes de Λ vue comme application à valeurs dans $(\mathbb{Z}/l\mathbb{Z})^r$.
On peut à nouveau raisonner comme dans 5.1 et on obtient

$$r_f + r_g + \#(\mathcal{F}_f) + \#(\mathcal{F}_g)$$

relations en décomposant $r_f + r_g + \#(\mathcal{F}_f) + \#(\mathcal{F}_g)$ éléments de $\mathcal{O}_f$ et de $\mathcal{O}_g$. Reste à résoudre le système associé dont les inconnues sont les logarithmes virtuels associés à Λ et l'on obtient $\log_\Lambda(\mathfrak{q})$ et $\log_\Lambda(\varepsilon_i)$ pour tout $\mathfrak{q}$ dans $\mathcal{F}_f \cup \mathcal{F}_g$ et tous générateurs des parties sans torsion de U_f et U_g.

5.3 Logarithme individuel

Soit Λ une application de Schirokauer. Pour $z \in \mathbb{F}_{p^n}^*$ on calcule le logarithme discret de z à l'aide du logarithme virtuel associé à Λ. D'après 5.1, on peut identifier $\mathbb{F}_{p^n}$ à $\mathbb{F}_p[m]$ et par suite, on peut écrire $z = \sum_{j=0}^{n} z_j m^j$ avec pour tout $j \in \{0, ..., n\}$, z_j un entier compris entre 0 et $p-1$. Notons $\hat{z} = \sum_{j=0}^{n} z_j \alpha^j$ un relevé de z dans $\mathcal{O}_f$. Si l'idéal $\hat{z}\mathcal{O}_f$ se décompose en idéaux premiers tous éléments de $\mathcal{F}_f$ alors $\hat{z}^h$ se décompose en un produit d'unités et d'éléments de la forme $\gamma_\mathfrak{q}$. Précisément on a:

$$\hat{z}^h = \varepsilon_0^{k_0} \prod_{i=1}^{r} \varepsilon_i^{k_i} \prod_{\mathfrak{q}\in\mathcal{F}_f} \gamma_\mathfrak{q}^{\mathrm{val}_\mathfrak{q}(\hat{z})}$$

où les $(k_i)_{0\leq i\leq r}$ sont des entiers relatifs. On obtient alors par ρ_f l'identité suivante :

$$\log(z) = \sum_{i=1}^{r} k_i \log_\Lambda(\varepsilon_i) + \sum_{\mathfrak{q}\in\mathcal{F}_f} \mathrm{val}_\mathfrak{q}(\hat{z})\log_\Lambda(\mathfrak{q}).$$

Remarque 5.7. *Il est nécessaire que l'idéal engendré par $\hat{z}$ se décompose selon $\mathcal{F}_f$. Si ce n'est pas le cas on élève z à une certaine puissance a prise au hasard, et on recommence jusqu'à ce que $\hat{z}^a$ vérifie la condition voulue, ce qui permet de conclure.*

6 Construction des corps de nombres

6.1 Rappel sur les résultants

Soit A un anneau commutatif et

$$P(X) = a_n X^n + \cdots + a_0 \text{ et } Q(X) = b_m X^m + \cdots + b_0$$

deux polynômes de $A[X]$. On définit la matrice de Sylvester $\mathrm{Syl}(P,Q)$ dans $M_{m+n}(A)$ associée à P et Q de la manière suivante : La première colonne de $\mathrm{Syl}(P,Q)$ est constituée des coefficients $(a_n, \ldots, a_0, 0, \ldots, 0)$.
La deuxième colonne des mêmes coefficients décalés d'un cran : $(0, a_n, \ldots, a_0, 0, \ldots, 0)$.
Pour la troisième colonne on recommence l'opération : $(0, 0, a_n, \ldots, a_0, 0, \ldots, 0)$.
De même jusqu'à la colonne m incluse.
La colonne m+1 est constituée des coefficients suivants : $(b_m, \ldots, b_0, 0, \ldots, 0)$.
On recommence l'opération de permutation circulaire pour les $n + m - 1$ colonnes suivantes et l'on obtient ainsi $\mathrm{Syl}(P,Q)$,

$$\mathrm{Syl}(P,Q) = \begin{pmatrix} a_n & 0 & \ldots & 0 & b_m & 0 & \ldots & \ldots & \ldots & 0 \\ a_{n-1} & a_n & \ldots & 0 & b_{m-1} & b_m & 0 & \ldots & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ \ldots & \ldots & \ldots & \ldots & b_0 & b_1 & \ldots & b_m & 0 & \ldots \\ a_0 & a_1 & \ldots & a_i & 0 & b_0 & \ldots & \ldots & \ldots & 0 \\ 0 & a_0 & \ldots & a_{i-1} & 0 & 0 & \ldots & \ldots & \ldots & b_m \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & a_0 & 0 & 0 & \ldots & \ldots & \ldots & b_0 \end{pmatrix}$$

Cette matrice est associée, dans les bases canoniques, à l'application :

$$S : A_{m-1}[X] \times A_{n-1}[X] \to A_{n+m-1}[X]$$

définie par :

$$S(A,B) = AP + BQ.$$

Définition 6.1. *Soit P et Q deux polynômes de $A[X]$, on appelle résultant de P et Q et l'on note* $\mathrm{res}(P,Q)$ *le déterminant de la matrice de Sylvester associée à P et Q.*

Si A est intègre de corps des fractions K, on a la proposition suivante :

Proposition 6.2. *Soit $P(X) = a_n X^n + \cdots + a_0$ et $Q(X) = b_m X^m + \cdots + b_0$ deux polynômes de $A[X]$ et* $\mathrm{res}(P,Q)$ *leur résultant. On note $(\alpha_1, \ldots, \alpha_n)$ (respectivement $(\beta_1, \ldots, \beta_m)$) les racines de P (respectivement Q) dans $\bar{K}$ avec multiplicité. On a alors :*

$$\mathrm{res}(P,Q) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j),$$

soit encore

$$\mathrm{res}(P,Q) = a_n^m \prod_{i\in\{1,\dots,n\}} Q(\alpha_i) = (-1)^{nm} b_m^n \prod_{j\in\{1,\dots,m\}} P(\beta_j).$$

Lemme 6.3. *Soient P, Q deux polynomes de $\mathbb{Z}[X]$ ayant un facteur commun modulo p. Alors $\mathrm{res}(P,Q)$ est un entier divisible par p.*

Preuve. Par définition le résultant est le déterminant de l'application

$$\mathbb{Z}_{m-1}[X] \times \mathbb{Z}_{n-1}[X] \longrightarrow \mathbb{Z}_{m+n-1}[X], \quad (A,B) \mapsto AP + BQ.$$

Donc le résultant s'annule si et seulement si P et Q ont un facteur commun. Par conséquent si P et Q ont un facteur commun modulo p, il s'en suit que $\mathrm{res}(P,Q)$ est un entier divisible par p. □

Lemme 6.4. *Le cas optimal en terme de complexité pour avoir un résultant $\mathrm{res}(P,Q)$ de l'ordre p avec des coefficients de P et Q les plus grands possibles en valeurs absolues est obtenu pour P, Q de même degré n,*

$$P(X) = a_n X^n + \cdots + a_0 \text{ et } Q(X) = b_n X^n + \cdots + b_0$$

avec $(a_i)_{0\le i\le n}$ et $(b_i)_{0\le i\le n}$ d'ordre $p^{1/2n}$

Preuve. Le résultant est le déterminant d'une matrice dont les coefficients s'identifient à ceux de P et Q. Ainsi

$$\mathrm{res}(P,Q) = \sum_{\sigma\in\mathfrak{S}m+n} \mathrm{sign}(\sigma) \prod_{i=1}^{m+n} c_{i,\sigma(i)} \tag{6.1}$$

où les $c_{i,\sigma(j)}$ sont pris parmis les coefficients $(a_k)_{k=0,\dots,n}$ et $(b_l)_{l=0,\dots,m}$ coefficients de P et Q. On en déduit, puisque $|\mathrm{res}(P,Q)|$ est au moins égale à p, que ces coefficients sont au moins d'ordre $p^{\frac{1}{n+m}}$ pour m et n négligeables devant p. D'où le lemme. □

6.2 Corps de nombres pour le crible

D'après §5.1,§5.2 et §5.3, le problème du logarithme discret se ramène à construire, deux extensions finies K_f et K_g de $\mathbb{Q}$ de même degré définies par des polynômes f et g dont les réductions modulo p ont un facteur irréductible commun sur $\mathbb{F}_p[X]$ de degré n. De plus, f et g doivent être choisis de façon à minimiser la complexité de l'algorithme associé. On a la proposition suivante :

Proposition 6.5. *Soit α une racine complexe de f, notons $c(f)$ le coefficient dominant du polynôme f. Soit φ un polynôme de $\mathbb{Z}[X]$, alors*

$$N(\varphi(\alpha)\mathcal{O}_f) = \pm c(f)^{-\deg(\varphi)} \mathrm{res}(f,\varphi).$$

Preuve. Par définition de la norme, $N(\varphi(\alpha)\mathcal{O}_f)$ est égal au produit des $\{\varphi(\alpha_i)\}_{1\leq i\leq n}$ où $\{\alpha_i\}_{1\leq i\leq n}$ désigne la famille des racines complexes de f. L'identité se déduit de la Proposition 6.2. □

D'après §5.1, pour collecter des relations sur les éléments de $\mathcal{F}_f$, on doit décomposer en idéaux premiers des idéaux principaux B-lisses de la forme $\varphi(\alpha)\mathcal{O}_f$ avec φ de degré inférieur ou égal à $t-1$. On effectue cette opération successivement sur une suite aléatoire de polynômes φ.

Soit β une racine complexe de g, il s'agit donc de maximiser la probabilité d'avoir $\varphi(\alpha)$ et $\varphi(\beta)$ générateurs d'idéaux B-lisses dans $\mathcal{O}_f$, respectivement $\mathcal{O}_g$. La norme étant multiplicative, pour maximiser ces probabilités, il faut contrôler $\mathrm{res}(f,\varphi)$ et $\mathrm{res}(g,\varphi)$ pour tout φ en fonction de f et g. C'est cette condition qui va guider la construction des polynômes f et g.
Pour majorer les résultants, on majore les coefficients des polynômes f et g. Rappelons que ces deux polynômes doivent être premiers entre eux sur $\mathbb{Q}$ avec pourtant un polynôme irréductible de degré n qui les divise sur $\mathbb{F}_p$. Par conséquent, $\mathrm{res}(f,g)$ différent de 0 et divisible par p (Lemme 6.3) et les coefficients de f et g sont en valeurs absolues de l'ordre de $p^{1/2n}$ (Lemme 6.4).

En résumé, on cherche des polynômes f et g irréductibles, premiers entre eux de degré n, de coefficients dans $\mathbb{Z}$ d'ordre $p^{1/2n}$ dont les réductions modulo p coïncident et sont irréductibles.
Nous rappelons ici, les constructions de polynômes f, g pertinents (mais ne satisfaisant pas la condition idéale sur la taille des coefficients) dues à Joux, Lercier ([JL]) pour le cas des corps premiers et à Joux, Lercier, Smart et Vercauteren en moyenne caractéristique ([JLSV]). Précisément,

Proposition 6.6. *On peut construire en temps polynomial deux polynômes f et g de $\mathbb{Z}[X]$ de degré n, irréductibles, avec f à coefficients dans $\{-1,0,1\}$ tels que f et g soit égaux modulo p.*

Preuve. Cette construction consiste à choisir un polynôme f de $\mathbb{Z}[X]$ à petits coefficients (dont les coefficients appartiennent à $\{1,-1,0\}$) irréductible modulo p et de degré n. Il suffit alors de prendre pour g le polynôme $f+p$. Le couple (f,g) vérifie alors les conditions voulues. □

Le défaut de cette construction vient de la taille des coefficients de g, de l'ordre de p. Une autre construction est proposée dans [JLSV]:

Proposition 6.7. *On peut construire en temps polynomial deux polynômes f et g de $\mathbb{Z}[X]$ de degré n, irréductibles, égaux modulo p et dont les coefficients sont plus petits en valeurs absolues que $\sqrt{p}$.*

Preuve. On construit f en posant $f=r+ch$ où r et h sont des polynômes de $\mathbb{Z}[X]$ à petits coefficients (tous éléments de $\{-1,0,1\}$) et c un entier de

l'ordre de $\sqrt{p}$ en valeur absolue. Les polynômes r et h et l'entier c sont choisis de telle sorte que f soit irréductible modulo p. On écrit alors c comme le rapport modulo p de deux entiers a et b d'ordre $\sqrt{p}$:

$$c = a/b \mod p.$$

On pose $g = br + ah$ polynôme de $\mathbb{Z}[X]$ irréductible modulo p et tel que

$$g \equiv bf \mod p.$$

□

La construction de [JLSV] (Proposition 6.7) a l'avantage de symétriser les rôles de f et g. Ils ont des coefficients du même ordre ($\sqrt{p}$), ils sont irréductibles et ont même degré. Cette construction joue un rôle important dans la mise en œuvre du crible multiple par corps de nombres. En effet le crible multiple par corps de nombres, initié par Barbulescu et Pierrot ([BP]) consiste à étudier non plus deux mais une famille de corps de nombres au dessus d'une extension de $\mathbb{F}_p$ fixée. Il est naturel, dans ce cas, de demander à ce que les corps nombres aient tous des propriétés analogues pour assurer l'amélioration du calcul d'indice.

Dans la partie suivante (6.3), on propose une construction nouvelle de f et g. Les polynômes obtenus par cette méthode sont candidats pour être de degré n, premiers entre eux, avec des coefficients de l'ordre de $p^{1/2n}$ et possédant modulo p une racine commune engendrant $\mathbb{F}_p$. Il convient néanmoins de signaler d'ores et déjà une faiblesse de cette construction. En effet, sa complexité étant exponentielle (§7), elle n'est pas utile en pratique. Trouver un algorithme produisant de tels f et g avec une complexité sous-exponentielle reste un problème ouvert.

6.3 Une construction nouvelle des corps de nombres

On commence par rappeler la méthode de Montgomery ([El]) et on en détaille la construction afin de pouvoir l'appliquer ensuite dans une situation analogue (§7).

Proposition 6.8. *On peut construire en temps polynomial deux polynômes f_1 et f_2 dans $\mathbb{Z}[X]$ de degré 2, premiers entre eux, possédant une racine commune θ dans $\mathbb{F}_p$ et des coefficients tous de l'ordre de $p^{1/4}$.*

Preuve. On choisit t et q dans $\mathbb{Z}$ tel que $p \equiv t^2 \mod q$ où q est d'ordre $\sqrt{p}$. On peut prendre par exemple $t = \lfloor\sqrt{p}\rfloor$ et q un diviseur de $p - (\lfloor\sqrt{p}\rfloor)^2$. Pour $(a, b, c) \in \mathbb{Z}^3$ tel que $aq + bt + c(t^2 - p)/q = 0$ le polynôme $a + bX + cX^2$ admet $t/q \mod (p)$ comme racine modulo p. Soit

$$E = \{(a, b, c) \in \mathbb{Z}^3 \text{ tel que } aq + bt + c(t^2 - p)/q = 0\}.$$

Le $\mathbb{Z}$-module E libre de rang 2 s'identifie au réseau orthogonal au vecteur $(q, t, (t^2-p)/q)$. Notons

$$M = \begin{pmatrix} q & t & (t^2-p)/q \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Ainsi, on a

$$(a,b,c) \in E \Longleftrightarrow \begin{pmatrix} 0 \\ a \\ b \\ c \end{pmatrix} \in \mathrm{Im}M.$$

On cherche les petites solutions pour $p^{1/4}$ de E, c'est-à-dire l'ensemble des triplets (a,b,c) de E tels que :

$$\sqrt{a^2+b^2+c^2} \leq p^{1/4}.$$

Pour $K \geq p^{1/4}$ (assez grand), on définit :

$$M_K = \begin{pmatrix} Kq & Kt & K(t^2-p)/q \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

En définissant le déterminant d'une matrice rectangulaire comme la racine carrée du déterminant du produit de cette matrice par sa transposée, on a

$$\det(M_K) \approx K\sqrt{q^2+t^2+((t^2-p)/q)^2}. \tag{6.2}$$

On réduit M_K dans $\mathcal{M}_{3,4}(\mathbb{Z})$ et l'on obtient une nouvelle matrice $M_{K\mathrm{red}} \in \mathcal{M}_{3,4}(\mathbb{Z})$ équivalente à M_K de la forme :

$$M_{K\mathrm{red}} = \begin{pmatrix} 0 & 0 & K \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix}.$$

Par construction, (a_1, b_1, c_1) et (a_2, b_2, c_2) (éléments de E) définissent deux polynômes premiers entre eux

$$f_1(X) = a_1 + b_1X + c_1X^2 \text{ et } f_2(X) = a_2 + b_2X + c_2X^2$$

tels que modulo p, ils aient une racine commune dans $\mathbb{F}_p$.
L'équivalence conservant le déterminant on a :

$$\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{vmatrix} K = \det(M_K).$$

Notons $u = (a_1, b_1, c_1)$ le vecteur à la norme euclidienne la plus grande entre (a_1, b_1, c_1) et (a_2, b_2, c_2). On obtient en minorant le déterminant de $\begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{vmatrix}$, l'inégalité suivante :

$$(\|u\|^4 - 2\|u\|^2)^{1/2} \leq \sqrt{q^2 + t^2 + ((t^2 - p)/q)^2} \approx \sqrt{p}. \tag{6.3}$$

Ainsi $\|u\| \leq p^{1/4}$. Les polynômes f_1 et f_2 ont une racine commune θ modulo p dans $\mathbb{F}_p$, sont premiers entre eux comme polynômes de $\mathbb{Z}[X]$ et ont des coefficients tous de valeurs absolues plus petites que $p^{1/4}$. □

Soient f_1 et f_2 deux polynômes premiers entre eux de $\mathbb{Z}[X]$ de degré deux de coefficients tous de valeurs absolues plus petites que $p^{1/4}$ ayant une racine commune θ modulo p dans $\mathbb{F}_p$ construits en suivant la proposition 6.8. Dans la suite on identifie θ à son relèvement dans $\mathbb{Z}$ compris entre 0 et $p-1$. Suivant la méthode du crible par corps de nombres (5.1), on déduit de la connaissance de ces deux polynômes, f_1 et f_2, un algorithme qui calcule le logarithme discret dans $\mathbb{F}_p$. Avec ces notations, nous allons à présent construire deux autres polynômes f et g permettant de définir un algorithme calculant le logarithme discret dans $\mathbb{F}_{p^n}$ (voir 5.1).

Soit $h \in \mathbb{Z}[X]$ irréductible dans $\mathbb{F}_p$ de degré n

$$h(X, \theta) = \sum_{i=0}^{n} h_i X^i \text{ avec } h_i = \pm 1 \pm \theta \text{ pour } 0 \leq i \leq n-1 \text{ et } h_n = 1.$$

Pour $0 \leq i \leq n$, on pose $h_i = h_i^0 + h_i^1 \theta$ avec $h_i^0 = \pm 1$ et $h_i^1 = \pm 1$. On note enfin

$$h^0(X) = \sum_{i=0}^{n} h_i^0 X^i, h^1(X) = \sum_{i=0}^{n} h_i^1 X^i, \text{ ainsi } h(X, \theta) = h^0(X) + h^1(X)\theta.$$

Pour trouver un polynôme h irréductible de cette forme, on procède comme suit : on choisit les coefficients h_i au hasard. On teste l'irréductibilité de h, par exemple en montrant via un calcul de résultant qu'il est premier avec $x^{p^k} - x$ pour tout k entre 1 et $n-1$. On obtient de la sorte un polynôme h irréductible. On rappelle le fait suivant qui suggère que cette stratégie est valide car il y a beaucoup de polynômes irréductibles de degré n dans $\mathbb{F}_p$:

Proposition 6.9. *La probabilité d'obtenir un polynôme irréductible de degré n à coefficients dans $\mathbb{F}_p$ parmi les polynômes de degré n est comprise entre $(1 - 1/p^{n/2-1})/n$ et $1/n$.*

Preuve. Tout élément de $\mathbb{F}_p^n$ est racine d'un polynôme irréductible unitaire de degré d divisant n. Un polynôme unitaire de degré d sur $\mathbb{F}_p$ s'identifie à son système de d racines. On déduit que $p^n = \sum_{d|n} d m_d(p)$ où $m_d(p)$ est

le cardinal des polynômes irréductibles unitaires de $\mathbb{F}_p[X]$ de degré d. On déduit donc l'encadrement suivant

$$\frac{p^n - p^{n/2+1}}{n} \leq m_n(p) \leq \frac{p^n}{n}. \quad \square$$

On construit à partir de h, deux nouveaux polynômes f, g de degré $2n$ dans $\mathbb{Z}[X]$ en posant :

$$f(X) = \mathrm{res}_\theta(h(X,\theta), f_1(\theta)) \text{ et } g(X) = \mathrm{res}_\theta(h(X,\theta), f_2(\theta)).$$

Ce qui donne après calcul du résultant (6.2) :

$$f(X) = f_1\Big(-\frac{h^0(X)}{h^1(X)}\Big)(h^1(X))^2 \text{ et } g(X) = f_2\Big(-\frac{h^0(X)}{h^1(X)}\Big)(h^1(X))^2.$$

Les polynômes $f \mod p$ et $g \mod p$ s'annulent en $m \in \mathbb{F}_{p^n}$ racine sur $\mathbb{F}_p$ de $h(X,\theta)$ d'après l'expression de f et g en termes de résultant. Ainsi $f \mod p$ et $g \mod p$ ont bien une racine commune m dans $\mathbb{F}_{p^n}$ tel que m soit génératrice de $\mathbb{F}_{p^n}$ sur $\mathbb{F}_p$. Les coefficients h_i^0 et h_i^1 étant tous égaux à plus ou moins un, les coefficients de f et g ont même taille que ceux de f_1 et f_2 et sont donc d'ordre $p^{1/4}$ d'après 6.3. Enfin, les polynômes f_1 et f_2 étant premiers entre eux et de degré 2 on vérifie que f et g sont eux aussi premiers entre eux de degré $2n$. Il n'y a pas de gain de complexité à utiliser cette méthode comme on le voit dans la section §8.

7 Méthode de Montgomery généralisée ?

L'objet de cette partie §7 est de déterminer deux polynômes de $\mathbb{Z}[X]$ de même degré n, premiers entre eux à petits coefficients, i.e de normes toutes plus petites que $p^{1/2n}$. On veut de plus que ces polynômes aient une racine commune dans $\mathbb{F}_p$. La connaissance de tels polynômes est en effet cruciale pour optimiser la complexité du crible par corps de nombres (§5.1). Pour cela, on généralise la méthode de Montgomery (§6.3).

Soit t, q et $(u_i)_{0\leq i\leq n}$ éléments de $\mathbb{Z}$ tels que p ne divise pas q. Si l'on a $(a_0, \ldots, a_n) \in \mathbb{Z}^{n+1}$ tel que

$$a_0(q^{n-1} - pu_0) + a_1(q^{n-2}t - pu_1) + a_2(q^{n-3}t^2 - pu_2) + \cdots$$
$$+a_{n-1}(t^{n-1} - pu_{n-1}) + a_n(t^n - pu_n)/q = 0$$

alors modulo p, le rationnel t/q est une racine de $a_0+a_1X+a_2X^2+\cdots+a_nX^n$. C'est pourquoi on considère l'ensemble des $n+1$-uplets

$$E = \left\{ \begin{array}{c} (a_0, \ldots, a_n) \in \mathbb{Z}^{n+1} \text{ tel que} \\ a_0(q^{n-1} - pu_0) + a_1(q^{n-2}t - pu_1) + a_2(q^{n-3}t^2 - pu_2) + \cdots \\ +a_{n-1}(t^{n-1} - pu_{n-1}) + a_n(t^n - pu_n)/q = 0 \end{array} \right\}$$

Le $\mathbb{Z}$-module libre E de rang n est le réseau orthogonal au vecteur

$$\left(q^{n-1} - pu_0, q^{n-2}t - pu_1, \ldots, (t^n - pu_n)/q\right)$$

dans $\mathbb{Z}^{n+1}$.

Soit $M = \begin{pmatrix} q^{n-1} - pu_0 & q^{n-2}t - pu_1 & \ldots & \ldots & (t^n - pu_n)/q \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & 1 \end{pmatrix}$.

Un $n+1$-uplet $(a_0, \ldots, a_n)$ est dans E si et seulement si $M \begin{pmatrix} a_0 \\ \ldots \\ a_n \end{pmatrix} = \begin{pmatrix} 0 \\ a_0 \\ \ldots \\ a_n \end{pmatrix}$.

Les polynômes recherchés ont une famille de coefficients éléments de E. Pour borner uniformément leurs normes, on introduit donc M_K défini de la manière suivante pour K un paramètre réel positif (assez grand) :

$$M_K = \begin{pmatrix} K(q^{n-1} - pu_0) & K(q^{n-2}t - pu_1) & \ldots & \ldots & K(t^n - pu_n)/q \\ 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \ldots & 1 \end{pmatrix}.$$

Comme élément de $M_{n+2,n+1}(\mathbb{Z})$, M_K est équivalente à une matrice $M_{K\text{red}}$ de la forme :

$$M_{K\text{red}} = \begin{pmatrix} 0 & \ldots & 0 & K \\ a_{0,0} & a_{0,1} & \ldots & a_{0,n} \\ a_{1,0} & a_{1,1} & \ldots & a_{1,n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n,0} & a_{n,1} & \ldots & a_{n,n} \end{pmatrix}.$$

On peut calculer le déterminant commun aux deux matrices M_K et $M_{K\text{red}}$ et l'on obtient l'identité suivante :

$$\det(M_K) = K\sqrt{(q^{n-1} - pu_0)^2 + \ldots + (t^n - pu_n)^2/q^2} = K \det(N_K)$$

pour

$$N_K = \begin{pmatrix} a_{0,0} & a_{0,1} & \ldots & a_{0,n-1} \\ a_{1,0} & a_{1,1} & \ldots & a_{1,n-1} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n,0} & a_{n,1} & \ldots & a_{n,n-1} \end{pmatrix}.$$

Par l'algorithme LLL (voir [Co] théorème 2.6.2), le plus petit vecteur pour la norme euclidienne de E, noté b_1 est tel que $\|b_1\| \leq 2^{(n-1)/4} \det(N_K)^{1/n}$ et le second plus petit vecteur b_2 vérifie $\|b_2\| \leq 2^{n/4} \det(N_K)^{1/n-1}$. Ainsi l'on obtient

Lemme 7.1. *Si* $\det(N_K)$ *est de l'ordre de* $p^{1/2}$*, la généralisation de la méthode de Montgomery permet de construire deux polynômes à coefficients de l'ordre de* $p^{1/2n}$ *possédant une racine commune dans* $\mathbb{F}_p$.

Il s'agit à présent de déterminer des coefficients t et les $(u_i)_{0\leq i\leq n-1}$ pour lesquels l'hypothèse du lemme 7.1 est satisfaite, i.e. $\det(N_K)$ est de l'ordre de $p^{1/2}$. On suppose $u_n = 0$ et $q = t^n$.

Lemme 7.2. *Pour $s \in \mathbb{Z}$, on note s_p le plus petit entier en valeur absolue tel que $s \equiv s_p \mod p$. Si*

$$\left\lfloor p^{1/(n(n-1))} \right\rfloor + 1 \leq t_p \leq p-1 \text{ et } ((t_p)^{(n-1)i})_p = (t^{(n-1)i})_p \leq p^{1/2}$$

alors la généralisation de la méthode de Montgomery produit deux polynômes b_1,b_2 sans racine commune évidente dans $\mathbb{Q}$ et de coefficients de l'ordre de $p^{1/2n}$.

Preuve. Sous les hypothèses du lemme, soient t et $(u_i)_{0\leq i\leq n-1}$ tels que $q^{n-i-1}t^i - pu_i$ soient de l'ordre de $p^{1/2}$ pour $0 \leq i \leq n$. Comme les deux polynômes associés à b_1 et b_2 n'ont pas de racines communes dans $\mathbb{C}$, on doit exclure les cas $0 \leq (t_p)^{n(n-1)} \leq p$. En effet, si $0 \leq (t_p)^{n(n-1)} \leq p$, alors t/q serait racine commune à b_1 et b_2 dans $\mathbb{Q}$. Ainsi $\left\lfloor p^{1/(n(n-1))} \right\rfloor + 1 \leq t_p \leq p-1$ avec $((t_p)^{ni})_p = (t^{ni})_p$. Alors, par division euclidienne, on en déduit b_1 et b_2 et les deux polynômes associés. □

Remarque 7.3. *Il reste à s'assurer que les deux polynômes construits par la méthode de Montgomery généralisée sont premiers entre eux. On peut tester ce fait par l'algorithme d'Euclide qui est polynomial en n^2 si n est le degré des deux polynômes. Complexité négligeable au vu des autres phases de l'algorithme du crible.*

Les limites de cette version généralisée de la méthode de Montgomery tient à la détermination de l'élément $t \in \mathbb{Z}$ satisfaisant les hypothèses du Lemme 7.2. Or, pour t_p quelconque, la probabilité pour un certain i d'avoir $(t^{ni})_p$ de l'ordre de $p^{1/2}$ est égale à $1/p^{1/2}$. Ainsi, pour t_p choisi au hasard la probabilité pour que pour tout $i \in [0, n]$ de telles conditions soient vérifiées est inférieure à $1/p^{n/2}$. D'où

Lemme 7.4. *La complexité de la généralisation de la méthode de Montgomery est exponentielle en* $\log(p)$.

Cette généralisation de la méthode de Montgomery permet donc en théorie de proposer des polynômes candidats aux conditions demandées (de degré n premier entre eux avec des coefficients d'ordre $p^{1/2n}$ avec une racine commune dans $\mathbb{F}_p$) mais en temps exponentiel ce qui n'est pas satisfaisant. Actuellement on ne sait pas s'il existe une variante de la méthode de Montgomery qui détermine en temps raisonnable deux polynômes satisfaisant toutes les hypothèses requises.

8 Calcul de Complexité

En grande caractéristique, le crible par corps de nombres par la méthode de Joux-Lercier ([JL]) utilisée seule est de complexité asymptotique minimale

$\mathrm{L}_{p^n}(1/3,(64/9)^{1/3})$ pour la détermination du logarithme discret d'un élément d'un corps fini $\mathbb{F}_{p^n}$. On ne donne dans cette partie §8 que le calcul de complexité dans le cas limite entre moyenne et grande caractéristique pour la construction des corps de nombres de la partie §6.3.

Rappelons les notations pour $\mathbb{F}_{p^n}$ pour cette caractéristique :

$$q = p^n \text{ et } p = \mathrm{L}_q(2/3, 1/\alpha_n)$$

où α_n est un réel de l'ordre de 1. D'après la définition de la fonction L (voir §3.3), on a donc

$$n = \alpha_n(\log(q)/\log(\log(q)))^{1/3}.$$

Soit B la borne de lissité, on définit le réel α_B par l'égalité

$$B = \mathrm{L}_q(1/3, \alpha_B).$$

Notons C la taille (i.e. le nombre d'éléments) du crible. On suppose que $C = B$. On restreint le crible aux éléments de la forme $a + b\alpha$ et $a + b\beta$ où a et b sont des entiers naturels plus petits que B et α et β sont les générateurs respectifs des corps K_f et K_g construits dans la section §6.3. La norme d'un élément $x \in K_f$ (resp. K_g) peut aussi s'écrire comme le produit des $\sigma(x)$ pour σ décrivant l'ensemble des plongements de K_f (resp. K_g) considéré dans $\mathbb{C}$.
On déduit des notations que

$$\mathrm{N}(a + b\alpha)\mathrm{N}(a + b\beta) \leq \mathcal{N} \text{ pour } \mathcal{N} = (n+1)^2 p^{1/2} B^{4n}.$$

On impose aux éléments du crible d'être tous B-lisses. D'après le théorème de Canfield-Erdos-Pomerance (Théorème 3.1) :

$$\log(\mathrm{P}(x \leq \mathcal{N} | B - lisse)) \approx -\frac{\log(\mathcal{N})}{\log(B)} \log(\frac{\log(\mathcal{N})}{\log(B)}). \tag{8.1}$$

Proposition 8.1. *Entre moyenne et grande caractéristique, le crible par corps de nombres sur* $\mathbf{F}_{p^n}$ *est de complexité asymptotique minimale de l'ordre de*

$$\mathrm{L}_{p^n}(1/3, (64/9)^{1/3}).$$

Preuve. La partie algèbre linéaire du crible par corps de nombres consiste à inverser une matrice de taille $B \times B$, donc a pour complexité B^2. Ainsi, pour égaliser les complexités de la partie "crible" (§8.1) et de la partie "algèbre linéaire" on doit avoir :

$$\log(\mathcal{N})\log(\frac{\log(\mathcal{N})}{\log(B)}) = \log^2(B).$$

Or $\mathcal{N} = (n+1)^2 p^{1/2} C^{4n}$, donc

$$\log^2 B = \Big(2\log(n+1)+(1/2)\log(p)+4n\log(B)\Big)\log\Big(2\log(n+1)+(1/2)\log(p)+4n\log(B)\Big).$$

On peut supposer $2\log(n+1)$ négligeable devant $4n\log(B)$ pour p^n grand. Ainsi, $\log(B)$ est solution de :

$$X^2 = ((1/2)\log(p) + 4nX)\log\Big((1/2)\log(p) + 4nX\Big).$$

On peut exprimer $\log(B)$ en fonction de α_B et n en fonction de α_n. Si l'on écrit de plus $\log(p) = \log(Q)/n$ on obtient :

$$\alpha_B(\log(Q)/\log(\log(Q)))^{1/3} =$$

$$2/3\alpha_n 2(\log(Q)/\log(\log(Q)))^{1/3} + (1/(6\alpha_B\alpha_n))(\log(Q)/\log(\log(Q)))^{1/3}.$$

Le facteur α_B est donc la racine positive de :

$$X^2 - 2/3\alpha_n 2X - 1/(6\alpha_n).$$

Par conséquent,

$$\alpha_B = \alpha_n 2/3 + \sqrt{\alpha_n^2 4/9 + 1/(6\alpha_n)}. \tag{8.2}$$

La complexité étant égale à B^2 et $B = \mathrm{L}_q(1/3, \alpha_B)$, on obtient une expression de la complexité en fonction de α_n. Elle est minimale pour α_B minimal en fonction de α_n. On cherche donc les zéros de la dérivée de l'expression précédente (§8.2) en fonction de α_n :

$$2/3 + \frac{8/9\alpha_n - 1/(6\alpha_n^2)}{2(\alpha_n^2 4/9 + 1/(6\alpha_n))^{1/2}} = 0.$$

On en déduit α_n que l'on peut remplacer dans :

$$X^2 - 2/3\alpha_n 2X - 1/(6\alpha_n)$$

où l'inconnu est α_B. Ce binôme ne possède qu'une racine positive, α_B :

$$\alpha_B = (2/3)(3)^{1/3}.$$

Par suite, la complexité asymptotique minimale est de l'ordre de :

$$\mathrm{L}_{p^n}(1/3, (64/9)^{1/3}).$$

□

La complexité du crible par corps de nombres entre moyenne et grande caractéristique (Proposition 8.1) est donc identique à celle obtenue par la méthode de Joux-Lercier (voir [JLSV]). Le gain en terme de taille des coefficients des polynômes - d'ordre $p^{1/2}$ dans la méthode de Joux-Lercier et d'ordre $p^{1/4}$ avec la construction §6.3- est balancé par l'augmentation des degrés des polynômes - de degré n dans le cas Joux-Lercier et de degré $2n$ pour §6.3.- Ces deux distinctions se compensent et l'on obtient la même complexité pour les deux algorithmes.

9 Entre la petite et la moyenne caractéristique

En petite caractéristique (§4), c'est-à-dire pour p de la forme

$$p = \mathrm{L}_{p^n}(\alpha, c) \text{ avec } \alpha \leq 1/3,$$

la complexité de l'algorithme par crible sur les corps de fonctions est meilleure que celle donnée par le crible par corps de nombres. Cette complexité est de l'ordre de $L_{p^n}(\alpha, c')$, pour un réel c' dépendant de α et c. Il est naturel de regarder le cas limite, i.e pour $\alpha = 1/3$ et c est variable et croissant. De la sorte, on approche de la fenêtre à partir de laquelle l'algorithme optimal de calcul de logarithme discret est obtenu à l'aide du crible par corps de nombres. D'après la section 10), le meilleur algorithme à ce jour pour $\alpha > 1/3$ est de complexité

$$\mathrm{L}_{p^n}(1/3, (48/9)^{1/3})$$

pour certains n ("divisible par une petite constante"). L'objet de cette section §9 est l'analyse de la complexité du crible par corps de nombres pour $\alpha = 1/3$. On commence par montrer que l'analyse analogue au cas $\alpha > 1/3$ ne s'applique pas (§9.1). Une majoration plus fine du déterminant de Sylvester s'avère nécessaire (§9.2).

9.1 Complexité entre petite et moyenne caractéristique

On rappelle les notations du crible par corps de nombres (§5.1):
- $t - 1$ le degré des polynômes du crible,
- B la borne de lissité,
- A la borne sur les coefficients des différents polynômes du crible.

Comme $p = \mathrm{L}_{p^n}(\alpha, c)$ avec $\alpha \leq 1/3$, on a

$$n = \frac{1}{c_p}\Big(\frac{\ln(q)}{\ln(\ln(q))}\Big)^{2/3}.$$

Ecrivons t sous la forme :

$$t = \frac{c_t}{c_p}\Big(\frac{\ln(q)}{\ln(\ln(q))}\Big)^{1/3}.$$

On peut aussi exprimer A^t et B sous les expressions suivantes (voir [JP]) :

$$A^t = \mathrm{L}_q(1/3, c_a c_t) \qquad \text{et} \qquad B = \mathrm{L}_q(1/3, c_b)$$

pour c_a, c_b deux réels.

La complexité de l'algorithme par corps de nombre dépend de la norme des polynômes du crible dans chacun des deux corps de nombres (§6.3). Cette norme, à un coefficient négligeable au vu de leurs tailles, est de l'ordre de :

$$\det(\mathrm{Syl}(f_i, h))$$

où $\mathrm{Syl}(f_i, h)$ est la matrice de sylvester associée aux polynômes f_i et h.

Lemme 9.1. *Notons $\|f_i\|$ le maximum des valeurs absolues des coefficients de f_i et A une borne de la valeur absolue des coefficients de h, alors*

$$|\mathrm{res}(f_i, h)| \leq n^m m^n A^n \|f_i\|^t .$$

Preuve. Vue la forme de la matrice de Sylvester $\mathrm{Syl}(f_i, h) = (c_{ij})_{0 \leq i \leq n+m-1}$, le nombre de permutations $\sigma \in \mathfrak{S}_{n+m}$ qui induisent un produit $\Pi_{i=0}^{m+n-1} c_{i,\sigma(i)}$ non nul dans l'expression développée (§6.1) du résultant est majoré par $n^m m^n$. □

Pour p de la forme $\mathrm{L}_q(\alpha, c)$ avec $\alpha > 1/3$, le terme $n^t t^n$ est négligeable devant $A^n \|f_i\|^t$. Il n'apparaît donc pas dans le calcul de complexité en moyenne et grande caractéristique.
Ce n'est plus le cas pour $\alpha = 1/3$ car t^n n'est plus négligeable. La majoration évidente de $|\mathrm{res}(f_i, h)|$ ne suffit plus pour retrouver la même complexité par le même calcul que dans le cas de moyenne caractéristique où $\alpha > 1/3$.

9.2 Majoration d'un résultant

Soient $P(X)$ et $Q(X)$ deux polynômes de degrés respectifs n et m avec $n \geq m$ et soit $\mathrm{Syl}(P, Q) = (m_{i,j})_{0 \leq i,j \leq n+m-1}$ la matrice de Sylvester associée. Ainsi

$$\mathrm{res}(P, Q) = \det \mathrm{Syl}(P, Q) = \sum_{\sigma \in \mathfrak{S}_{n+m}} \epsilon(\sigma) \prod_{k=0}^{n+m-1} m_{\sigma(k),k}.$$

On a donc la majoration évidente

$$|\mathrm{res}(P, Q)| \leq |\Theta| A^{n+m}$$

où $A = \max\{|m_{i,j}|, i, j \in \{0, \ldots, n+m-1\}\}$ et $|\Theta|$ est le cardinal de l'ensemble

$$\Theta = \{\sigma \in \mathfrak{S}_{n+m} \text{ tel que } \prod_{k=0}^{n+m-1} m_{\sigma(k),k} \neq 0\}.$$

On cherche à estimer $|\Theta|$ pour obtenir une approximation plus fine que dans le lemme 9.1 de $|\mathrm{res}(P, Q)|$. Pour ce faire, on utilise la forme particulière de la matrice de Sylvester qui contient beaucoup de coefficients nuls répartis de façon régulière. De plus il existe une césure dans cette matrice à la colonne m : on passe des coefficients de P aux coefficients de Q, ce qui permet de différencier les rôles des deux polynômes.

Lemme 9.2. *Pour $\sigma \in \mathfrak{S}_{n+m}$, posons*

$$l(\sigma) = \mathrm{Max}_{0 \leq j \leq m-1}(\sigma(j)).$$

Alors $l(\sigma) \geq m$.

Preuve. L'opérateur σ est une bijection. L'entier $l(\sigma)$ est le maximum d'un ensemble d'entiers naturels de cardinal strictement égal à m. D'où $l(\sigma) \geq m$. □

Lemme 9.3. *Soit $\sigma \in \Theta$. Alors σ induit une permutation de $\{0, \ldots, l(\sigma)\}$.*

Preuve. Par définition (§9.2), si $0 \leq j \leq m-1$ on a $\sigma(j) \leq l(\sigma)$. Soit $i \in [m, l(\sigma)]$. Si $\sigma(i) \geq l(\sigma)$, comme $i \leq l(\sigma)$, le coefficient $m_{\sigma(i),i}$ est situé strictement en dessous de la diagonale et dans la partie de la matrice associée à Q, donc est nul et $\sigma \notin \Theta$. □

A présent, il est naturel d'étudier $\sigma(k)$ pour k supérieur à l. On a la proposition suivante :

Proposition 9.4. *Soit $\sigma \in \Theta$ est non nulle. Alors pour tout $k > l(\sigma)$, on a $\sigma(k) = k$.*

Preuve. On raisonne par récurrence. Pour $k = l(\sigma)+1$. Les seules permutations éléments de Θ sont telles que $\sigma(l(\sigma)+1) \geq l(\sigma)+1$ d'après le lemme 9.3. Or dans ce cas le terme associé dans la matrice, $m_{\sigma(l(\sigma)+1),l(\sigma)+1}$ se situe sous la diagonale après la colonne m. Vue la forme de la matrice, il est non nul si et seulement si $\sigma(l(\sigma)+1) = l(\sigma)+1$.
Soit $u \geq l(\sigma)$. On suppose à présent que pour tout k compris entre $l(\sigma)+1$ et u, $\sigma(k) = k$. Comme σ est bijective, $\sigma(u+1) > l(\sigma)$. De plus en utilisant l'hypothèse de récurrence il vient que $\sigma(u+1) > u$. A nouveau les seuls termes possibles pour $\sigma(u+1)$ sont tels que $m_{\sigma(u+1),u+1}$ se situe au dessous de la diagonale dans une partie de la matrice (après la colonne m) où tous les termes strictement sous la diagonale sont nuls. Donc $\sigma(u+1) = u+1$ et la récurrence est établie au rang $u+1$. □

D'après la proposition 9.4, si $\sigma \in \Theta$ alors pour tout k tel que $l(\sigma)+1 \leq k \leq n+m-1$, on a $\sigma(k) = k$. Le polynôme $Q(X) = \sum_{i=0}^{m} b_i X^i$ est unitaire, i.e. $b_m = 1$. Donc pour $\sigma \in \Theta$ et k compris entre $l(\sigma)+1$ et $n+m-1$ on a : $m_{\sigma(k),k} = m_{k,k} = b_m$. On en déduit la majoration suivante de $|\mathrm{res}(P,Q)|$:

Proposition 9.5. *Soient P et Q deux polynômes unitaires de degré respectif n et m.*

$$|\mathrm{res}(P,Q)| \leq \sum_{\sigma \in \mathfrak{S}_{n+m}} \prod_{k=0}^{0 \leq j \leq \max\{l(\sigma),\sigma(j)\}} \left| m_{\sigma(k),k} \right|.$$

On donne une majoration du cardinal de Θ, i.e du nombre de permutations intervenant dans le résultant.

Lemme 9.6. *Soit P et Q deux polynômes de $\mathbb{Z}[X]$ de degré respectif n et m. Alors :*

$$|\Theta| \leq 2^{n+m}(n+1)!(m-1)!$$

Preuve. Il suffit de majorer le nombre de permutations évitant les coefficients nuls de la matrice de Sylvester associée à P et Q. Pour $\sigma(1)$, on a deux choix. Pour $\sigma(2)$ on a quatre choix et ainsi de suite jusqu'à $\sigma(n+1)$. Puis pour $\sigma(n+2)$ on a $2(m-1)$ choix, pour $\sigma(n+3)$, $2(m-2)$ choix et ainsi de suite jusqu'à $\sigma(n+m)$ où l'on a à nouveau deux choix. Ainsi, on obtient la majoration annoncée.

$$|\Theta| \leq 2^{n+m}(n+1)!(m-1)!$$

□

La majoration du lemme 9.6 est grossière et ne suffit pas à abaisser la complexité de l'algorithme du calcul d'indice entre la petite et la moyenne caractéristique. Il faut faire un travail plus fin, tenant compte de la signature des permutations de Θ et des coefficients de P et Q. En étant plus soigneux, on s'aperçoit que l'approximation de la valeur du résultant peut être l'objet de questions combinatoires ouvertes fines.

10 Variantes du crible par corps de nombres

Dans cette section §10, on présente deux variantes récentes du crible par corps de nombres. Elles sont indépendantes et peuvent être appliquées ensemble.

La première (§10.1), appelée crible multiple de corps de nombres, est due à Barbulescu et Pierrot ([BP]). Elle consiste à considérer plusieurs anneaux d'entiers au dessus d'un corps fini fixé. Elle augmente ainsi les relations linéaires entre logarithmes virtuels définies cette fois dans plus de deux corps de nombres. Elle permet de la sorte de faire baisser la complexité globale de l'algorithme de calcul d'indice associé.
La seconde variante (§10.2), dite méthode de crible par tour de corps de nombres, est due à Barbulescu et Kim ([BK]). Elle permet d'obtenir en moyenne caractéristique, les résultats de complexité obtenus pour la grande caractéristique. Elle consiste à tensoriser le diagramme du crible par corps de nombres classique pour $\mathbb{F}_{p^\eta}$ par un anneau d'entiers non ramifié en p de dimension κ. On obtient un algorithme global calculant le logarithme discret dans $\mathbb{F}_{p^n}$ où $n = \eta\kappa$ avec une complexité ne dépendant que de la caractéristique de $\mathbb{F}_{p^\eta}$.

10.1 Crible multiple par corps de nombres

Initiée par Barbulescu et Pierrot ([BP]), cette méthode consiste à multiplier le nombre d'anneaux d'entiers au dessus d'un corps fini fixé. Le crible par corps de nombres ne considère originellement que deux anneaux des entiers (5.1). Ici on multiplie le nombre d'égalités de la forme (2.1) sans avoir

à décomposer un trop grand nombre d'idéaux de la forme $\varphi(\alpha)\mathcal{O}_f$ dans les anneaux d'entiers $\mathcal{O}_f$.
Cependant, en multipliant les anneaux d'entiers au dessus d'un corps fini fixé, on augmente le temps de calcul de factorisation, dans chacun de ces anneaux d'entiers, en idéaux principaux. Par conséquent, il existe un nombre optimal d'anneaux d'entiers au dessus du corps fini.
La section §10.1 présente brièvement cette stratégie nouvelle due à Barbulescu et Pierrot. D'abord (§10.1.1), on indique la construction de ces anneaux d'entiers. Puis on détermine le nombre optimal d'anneaux d'entiers à considérer simultanément dans l'algorithme de crible multiple par corps de nombres (§10.1.2).

10.1.1 Famille d'anneaux d'entiers

D'après §6.2, on sait construire des couples de polynômes tels que leurs corps de rupture sur $\mathbb{Q}$ définissent des anneaux d'entiers répondant aux exigences du crible par corps de nombres (§6.2).

Pour construire non plus deux mais une famille de tels anneaux d'entiers, on prend des combinaisons linéaires des deux polynômes de départ :

$$\lambda f + \mu g$$

où λ et μ sont des entiers négligeables devant les coefficients de f et g. On obtient de la sorte des polynômes qui ont tous une racine commune sur $\mathbb{F}_p$ et l'on choisit dans cette famille de combinaisons linéaires, celles qui définissent des polynômes irréductibles. En agissant de la sorte, on symétrise les rôles des deux polynômes initiaux qui forment la base du $\mathbb{Z}$-module libre de rang 2 des polynômes candidats pour définir le crible multiple. Ils ont même degré et même taille.

L'optimisation de l'algorithme par crible multiple nécessite une limitation du nombre des polynômes à considérer. La borne est une constante négligeable devant la taille des deux polynômes originaux que nous explicitons dans le paragraphe suivant (§10.1.2).

10.1.2 Cardinal optimal de la famille associée au crible multiple

On adapte au crible multiple les notations de la section §5.1 du crible par corps de nombres. La méthode du crible repose sur la collection de relations linéaires entre logarithmes virtuels par décomposition des éléments du crible en produit d'idéaux premiers. Dans le cadre du crible multiple, on note V le nombre d'anneaux d'entiers de corps de nombres $(\mathbb{Q}[\alpha_i])_{1\leq i\leq V}$ au dessus du corps $\mathbb{F}_{p^n}$ étudié. Notons $(f_i)_{1\leq i\leq V}$ les polynomes minimaux respectifs de $(\alpha_i)_{1\leq i\leq V}$ et $\mathcal{O}_{f_i}$ l'anneau d'entiers de $\mathbb{Q}[\alpha_i]$. On obtient une relation linéaire

utile au crible lorsque que deux idéaux parmis la famille des $(\varphi(\alpha_i)\mathcal{O}_{f_i})_{1\leq i\leq V}$ sont B-lisses.

Notons $\mathcal{P}$ la probabilité pour un polynôme de degré inférieur strictement à un entier t d'être B-lisse dans une extension de la forme $\mathbb{Q}[\alpha_i]$. La probabilité pour un polynôme φ de degré inférieur strictement à t d'être B-lisse dans deux extensions de la forme $\mathbb{Q}[\alpha_i]$ est égale à

$$\mathcal{P}' = V(V-1)/2\mathcal{P}^2.$$

Ainsi la probabilité de construire une relation linéaire utile au crible est augmentée d'un facteur de l'ordre de V^2.

D'après [BP], les variables intervenant dans la complexité globale de l'algorithme sont :
- t la borne des degrés des polynômes sur lesquels on effectue le crible,
- S la taille maximale des coefficients de ces polynômes,
- B la borne de lissité du crible,
- V le nombre d'extensions de $\mathbb{F}_{p^n}$.

Comme dans le calcul de complexité de crible par corps de nombres (§8), on égalise la complexité des deux phases du crible : celle de collection des relations et celle d'algèbre linéaire. La phase de collection nécessite l'analyse de la B-lissité des S^t éléments du crible. La partie algèbre linéaire, via l'algorithme de Wiedemann ([Wi]), est de complexité de l'ordre de $(VB)^2$. On obtient ainsi

$$S^t = (VB)^2.$$

Pour la collection des VB relations nécessaires, on obtient une complexité

$$S^t\mathcal{P}' = VB.$$

Donc VB de l'ordre de $1/\mathcal{P}'$, pour $\mathcal{P}' = V(V-1)/2\mathcal{P}^2$. Ces relations déterminent V en fonction de B et $\mathcal{P}$.
Barbulescu et Pierrot mènent à bien les calculs de complexité en moyenne et grande caractéristique pour le crible multiple ([BP]) pour les paramètres $V, B, \mathcal{P}'$ ainsi choisis :

Proposition 10.1. *En moyenne caractéristique, la méthode du crible multiple conduit à une complexité égale à :*

$$\mathrm{L}_{p^n}(1/3, (2^{13}/3^6)^{1/3}).$$

En grande caractéristique, la méthode du crible multiple conduit à une complexité égale à :

$$\mathrm{L}_{p^n}(1/3, (\frac{92+26\sqrt{13}}{27})^{1/3}).$$

On rappelle que le crible par corps de nombres ([JL]) a pour complexité en moyenne caractéristique :

$$\mathrm{L}_{p^n}(1/3, (128/9)^{1/3})$$

or

$$(2^{13}/3^6)^{1/3} \cong 2,24 \text{ et } (128/9)^{1/3} \cong 2,42$$

d'où le gain escompté du crible multiple dans le cas de la moyenne caractéristique.
En grande caractéristique, le crible par corps de nombres ([JL]) a pour complexité

$$\mathrm{L}_{p^n}(1/3, (64/9)^{1/3}).$$

Or

$$(\frac{92+26\sqrt{13}}{27})^{1/3} \cong 1,902 \text{ et } (64/9)^{1/3} \cong 1,923.$$

Ainsi le crible multiple conduit à un gain en complexité que ce soit en grande ou en moyenne caractéristique.

Entre moyenne et grande caractéristique, i.e. pour

$$p = \mathrm{L}_{p^n}(2/3, c_p)$$

où c_p est un réel positif de l'ordre de 1 (il suffit ici de prendre c_p inférieur à 10). Dans ce cas la complexité dépend de c_p et de t. Précisément on a ([BP]) :

Proposition 10.2. *La complexité de l'algorithme de calcul d'indice avec le crible multiple pour*

$$p = \mathrm{L}_{p^n}(2/3, c_p)$$

et c_p de l'ordre de 1, est égale à :

$$\mathrm{L}_{p^n}\Big(1/3, 2/3(\frac{16}{9c_pt} + \sqrt{(\frac{16}{9c_pt})^2 + \frac{8}{3}(c_p(t-1))})\Big).$$

Rappelons la complexité de l'algorithme de calcul d'indice par la méthode de Joux-Lercier :

$$\mathrm{L}_{p^n}\Big(1/3, 2/3(\frac{2}{c_pt} + \sqrt{(\frac{2}{c_pt})^2 + 3(c_p(t-1))})\Big).$$

Ainsi on constate un gain de complexité via la mise en œuvre du crible multiple (10.2).

10.2 Crible par tour de corps de nombres

Dans cette section (§10.2), on donne une variante due à Barbulescu et Kim ([BK]), dite crible par tour de corps de nombres, du crible par corps de nombres. On commence par présenter le gain de complexité (Proposition 10.3), puis on décrit précisément la méthode de Barbulescu et Kim.

L'objectif du travail de Barbulescu et Kim ([BK]) est d'obtenir (sous des hypothèses que l'on précise dans la proposition 10.3) en moyenne caractéristique, une complexité équivalente au cas de grande caractéristique. Les calculs de complexité en grande caractéristique sont détaillés dans [JLSV]. Quelque soit la méthode utilisée, la complexité en grande caractéristique est inférieure à la complexité en moyenne caractéristique. Notamment la méthode de Joux-Lercier donne en grande caractéristique une complexité égale à $\mathrm{L}_{p^n}(1/3, (64/9)^{1/3})$ et en moyenne caractéristique $\mathrm{L}_{p^n}(1/3, (128/9)^{1/3})$. La méthode de Barbulescu et Kim (§[BK]) que l'on présente ici (10.2) permet d'obtenir la même constante, $(64/9)^{1/3}$, en grande et moyenne caractéristique. Elle permet de faire un peu plus. En effet, le cas limite entre moyenne et grande caractéristique, pour

$$p = \mathrm{L}_{p^n}(2/3, c_p)$$

avec c_p un réel positif de l'ordre de 1 (ici, il suffit de prendre c_p compris entre $0,1$ et 10) donne dans les cas optimaux une meilleure complexité qu'en grande caractéristique ([BK]) :

Proposition 10.3. *Soit $n = \eta\kappa$ et $q = p^n$. On suppose η et κ premiers entre eux et*

$$\eta = o\left(\left(\frac{\log q}{\log\log q}\right)^{1/3}\right).$$

Alors l'algorithme de calcul d'indice pour $\mathbb{F}_{p^n}$ associé à la méthode de crible par tour de corps de nombre a pour complexité

$$\mathrm{L}_{p^n}(1/3, (48/9)^{1/3}).$$

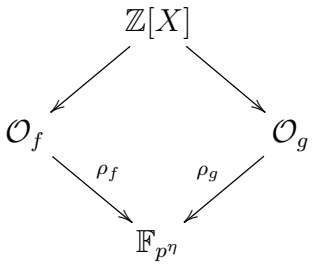
Décrivons à présent la méthode du crible par tour de corps de nombres. Soit $\mathbb{F}_{p^n}$ un corps de moyenne caractéristique avec $n = \eta\kappa$ tel que $\mathbb{F}_{p^\eta}$ est un extension entre moyenne et grande caractéristique.

D'après §6.3 la probabilité d'obtenir un polynôme irréductible unitaire sur $\mathbb{F}_p$ de degré κ est égale à $(1/\kappa)(1 - 1/p)$. Probabilité suffisamment grande (κ est inférieur à $\log(p^\kappa)$) pour qu'on puisse déterminer un tel polynôme, en temps polynomial en les variables (le nombre de chiffres nécessaire à l'écriture de p^κ). Quitte à prendre des relevés dans $\mathbb{Z}$ de ses coefficients, on construit ainsi un polynôme P irréductible unitaire de degré κ sur $\mathbb{Z}$ qui reste irréductible modulo p.
Soit ι une racine complexe de P, $\mathbb{Q}[\iota]$ l'extension de $\mathbb{Q}$ engendrée par ι et $\mathcal{O}_\iota$

l'anneau des entiers de $\mathbb{Q}[\iota]$. Comme P est irréductible modulo p, le nombre premier p est non ramifié dans $\mathcal{O}_\iota$. Par réduction modulo p, on obtient un morphisme surjectif d'anneaux :

$$\mathcal{O}_\iota \to \mathbb{F}_{p^\kappa}.$$

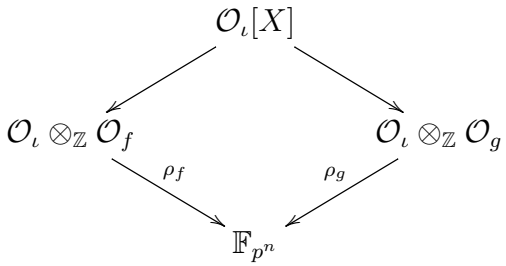
L'extension $\mathbb{F}_{p^\eta}$ est de grande caractéristique (ou entre moyenne et grande caractéristique). Le crible par corps de nombres usuel (§5.1) conduit au diagramme de réductions successives suivant :



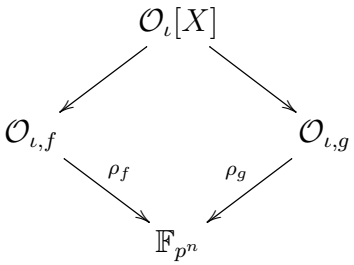
où f et g sont des polynômes introduits dans la section §6.2. On peut alors tensoriser sur $\mathbb{Z}$ ce diagramme par $\mathcal{O}_\iota$. En constatant que

$$\mathcal{O}_\iota \otimes_{\mathbb{Z}} \mathbb{F}_{p^\eta} = \mathbb{F}_{p^n},$$

on en déduit le diagramme suivant :



Cependant les anneaux $\mathcal{O}_\iota \otimes_{\mathbb{Z}} \mathcal{O}_f$ et $\mathcal{O}_\iota \otimes_{\mathbb{Z}} \mathcal{O}_g$ ne sont pas forcément de Dedekind. Il convient donc de travailler plutôt dans l'anneau $\mathcal{O}_{\iota,f}$ (respectivement $\mathcal{O}_{\iota,g}$) des entiers de l'extension $K_f[\iota]$ (respectivement $K_g[\iota]$). On obtient ainsi un nouveau diagramme :



Reste à collecter des relations et définir les ensembles d'idéaux B-lisses dans ces anneaux. On peut supposer que les coefficients du polynôme P

négligeables devant ceux de f et g. Les normes (sous les hypothèses de la proposition 10.3) restent alors du même ordre par passage de K_f ou K_g à $K_f[\iota]$ ou $K_g[\iota]$, ce qui permet de conserver la même complexité du crible de $\mathbb{F}_{p^\kappa}$ à $\mathbb{F}_{p^n}$.

Remarquons enfin que les méthodes de crible multiple et de crible par tour de corps de nombres peuvent s'associer et conduisent ensemble à une nouvelle complexité en moyenne caractéristique. Cette complexité est la meilleure pour $\mathbb{F}_{p^n}$ avec $n = \eta\kappa$ tel que $\mathbb{F}_{p^\eta}$ est de caratéristique strictement comprise entre la moyenne et la grande caractéristique ([BK]).

Proposition 10.4. *Sous les hypothèses de la proposition 10.3, la complexité pour le calcul d'indice sur $\mathbb{F}_{p^n}$ vaut*

$$\mathrm{L}_{p^n}\left(1/3, \left(\frac{92+26\sqrt{13}}{27}\right)^{1/3}\right)$$

en combinant la méthode de tour par corps de nombres et le crible multiple.

References

[Ad1] L. Adleman, *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, In 20th Annual Symposium on Foundations of Computer Science, 1979

[Ad2] L. Adleman, *The function field sieve*, Algorithmic Number Theory, Volume 877, 2005, 108–121.

[BGGM] R. Barbulescu, P. Gaudry, A. Guillevic, F. Morain, *Improvements to the number field sieve for non-prime finite fields.* MATHEMATICS OF COMPUTATION Volume 72, Number 242, 2014, 953–967.

[BGJT] R. Barbulescu, P. Gaudry, A. Joux, E. Thomé, *A heuristic quasi-polynomial algorithm for discrete logarithm in Finite Fields of small characteristic.* EUROCRYPT, 2014, 1–16.

[BP] R. Barbulescu, C. Pierrot, *The multiple number field sieve for medium- and high-characteristic finite fields* LMS Journal of Computation and Mathematics / Volume 17 / Special Issue A / 2014, 230–246.

[BK] R. Barbulescu, T. Kim, *Extended tower number field sieve: A new complexity for medium prime case.* Cryptography e-print archive report 2015/1027, 2015.

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory.* Springer , 1991.

[CEP] E.R. Canfield, P. Erdos, C. Pomerance, *On a problem of Oppenheim concerning "'Factorisatio Numerorum"'* Journal of Number Theory **17**, 1983, 1–28.

[DH] W. Diffie, M. E. Hellman, *New directions in cryptography* IEEE Trans. Inform. Theory, IT-22, 1976, 644–654.

[El] R.M. Elkenbracht-Huizing, *An implementation of the number field sieve.* Technical Report NM-R9511, CWI, 1995.

[HP] M. Hellman, S. Pohlig, *An improved algorithm for computing logarithms over GF(p) and his cryptographic signifiance* IEEE Trans. Inform. Theory , **24**, 1978, 106–110.

[Jo] A. Joux, *Faster Index Calculus for the Medium Prime Case Application to 1175-bit and 1425-bit Finite Fields* EUROCRYPT . 2013, 177–193.

[JL] A. Joux, R. Lercier, *Improvements to the general number field sieve for discrete logarithms in prime fields. A comparison with the Gaussian integer method* Math. Comput. 72 no. 242, 2003, 953–967.

[JLSV] A. Joux, R. Lercier, N. P. Smart, F. Vercauteren, *The number field sieve in the medium prime case* Advances in cryptology CRYPTO 2006, Lecture Notes in Computer Science 4117, Springer, 2006, 326–344.

[JP] A. Joux, C. Pierrot, *The Special Number Field Sieve in F_{p^n}, Application to Pairing-Friendly Cnstructions* Cryptography ePrint Archive: Report 2013/582.

[Kr] M. Kraitchik, *Théorie des nombres*, Gauthier-Villars, 1922.

[LO] B. A. LaMacchia, A. M. Odlyzko, *Computation of discrete logarithms in prime fields.* Designs, Codes and Cryptography, **1**, 1991, 47–62.

[Mu] B. Murphy, *Polynomial selection for the number field sieve. Integer factorisation algorithm*, Thèse 1999.

[Sc1] O. Schirokauer, *Discrete logarithms and local units.* Philos. Trans. Roy. Soc. London Ser. A, 345(1676), 1993, 409–423.

[Sc2] O. Schirokauer, *Virtual logarithms.* Journal of Algorithms, 57(2), 2005, 140–147.

[Wi] D. Wiedemann, *Sovling sparse linear equations over finite fiedls.* IEEE trans. Inform. Theory **32**, 1986, 54–62.

Part II

Catégories multivariées en théorie de Hodge p-adique

11 Introduction et rappel

Soit K une extension finie de $\mathbb{Q}_p$ et G_K le groupe de Galois absolu de K. Depuis les travaux de Colmez et Fontaine ([CF]) on sait décrire les représentations galoisiennes de G_K en termes de (φ, Γ)-modules, le groupe Γ étant défini à partir de la tour d'extensions cyclotomiques de K. Cette approche, extrêmement fructueuse, a permis la démonstration d'une partie du programme de Langlands p-adique qui cherche à classifier les représentations galoisiennes de G_K en termes de représentations linéaires (voir les travaux de Berger, Breuil, Colmez, Kisin...). Dans [KR], Kisin et Ren ont montré qu'il était possible de remplacer la tour cyclotomique par n'importe quelle tour associée à une loi de Lubin-Tate. La catégorie de modules, dit de Kisin, obtenue de la sorte permet, entre autres, de décrire les réseaux stables sous l'action de G_K déduits de représentations cristallines de G_K.

Nous commençons par un rappel sur les lois de groupes formelles de Lubin-Tate §12. Puis, §13, nous généralisons les résultats de [KR] en augmentant le nombre de variables de l'anneau sur lequel se construit les modules de Kisin. On définit une version multivariée des modules "cristallins" de [KR] (13.2). L'introduction de plusieurs variables est motivée par l'espoir de remplacer le groupe Γ par un groupe p-adique plus grand permettant d'obtenir des informations complémentaires dans des situations plus générales. Cette stratégie est déjà émergente dans les travaux récents de Berger ([Be2]) et de Kedlaya ([Ke]).

Le développement de la théorie classique à la structure multivariable révèle différentes difficultés nouvelles que l'on a cherchées à mettre en évidence dans ce texte. Notamment pour obtenir une équivalence entre la catégorie de certains φ-modules multivariés et une catégorie adaptée de représentations cristallines, la généralisation de la stratégie mise en œuvre dans [KR] nécessite une version multivariée de la théorie des pentes. Malheureusement, pour le moment, on ne dispose que d'une version partielle multivariée des pentes de Kedlaya ([Ke]) qui est encore insuffisante. Même dans le cas classique avec une seule variable, sans la théorie des pentes de Kedlaya, on ne sait pas décrire explicitement les réseaux stables dans des représentations galoisiennes cristallines à partir des modules de Kisin.

Cette difficulté est la motivation principale de la seconde partie §14 où, suivant la stratégie développée par Genestier et Lafforgue en caractéristique positive ([GL]), on munit les φ-modules d'une structure supplémentaire, dite de Hodge-Pink, qui pourrait permettre de contourner la théorie des pentes de Kedlaya. La condition de tranversalité de Griffiths se substitue à l' étude des pentes. Il s'agit de définir les objets analogues à la théorie de Genestier-Lafforgue dans le contexte d'une tour associée à une loi de Lubin-Tate. Nous concluons en rappelant la stratégie de Genestier-Lafforgue dans le cadre

de la tour cyclotomique, stratégie qui pourrait servir de guide dans le cas d'une tour associée à une loi de Lubin-Tate. Nous mettons enfin en évidence quelques difficultés nouvelles qui apparaissent dans ce cadre.

Ce travail est le reflet de multiples discussions avec Eugen Hellmann à l'Institut de Mathématiques de Jussieu Paris-Rive Gauche puis au MSRI (Mathematical Sciences Research Institut) qui a guidé l'auteur au cœur des méandres de la théorie de Hodge p-adiques avec enthousiasme et précision.

12 Lois de groupes de Lubin-Tate et notations

12.1 Rappel sur les lois de groupes de Lubin-Tate

On s'appuie essentiellement sur [We] dans cette partie. Soit A un anneau commutatif et $\mathcal{C}$ la catégorie des A-algèbres commutatives A' complètes pour un certain idéal I de A'. Soit $\mathcal{E}$ la catégorie des ensembles. Pour tout n entier, on peut définir le foncteur

$$\hat{\mathbb{A}}_A^n : \mathcal{C} \to \mathcal{E}$$

qui à A' associe l'ensemble des n-uplets de A' d'éléments topologiquement nilpotents pour la topologie I-adique de A'. Ce foncteur est représentable et est représenté par $A[[X_1, ..., X_n]]$ muni de la topologie $(X_1, ..., X_n)$-adique.

Définition 12.1. *On appelle Lie-Variété formelle de dimension n sur A tout foncteur $F : \mathcal{C} \to \mathcal{E}$ isomorphe à $\hat{\mathbb{A}}_A^n$. On la note $\mathcal{L}_f(A)^n$. L'union de ces espaces pour tout n est notée $\mathcal{L}_f(A)$.*

L'espace $\mathcal{L}_f(A)$ est muni d'une structure de catégorie. Ses objets sont les Lie-Variétés formelles et ses morphismes sont les morphismes de foncteurs définissant ces objets. Cette catégorie admet des objet-groupes G. En effet, elle est à produit fini (on passe alors des dimensions n et n' à la dimension $n + n'$ avec comme objet final le foncteur vide). Soit G un tel objet. Par construction il existe $n \in \mathbb{N}$ et φ un isomorphisme de $\mathcal{C}$ tel que G soit isomorphe par φ à un objet-groupe supporté par $\hat{\mathbb{A}}_A^n$.

Définition 12.2. *On appelle loi de groupe formelle sur A de dimension n tout objet-groupe commutatif sur $\mathcal{L}_f(A)$ d'espace sous jacent $\hat{\mathbb{A}}_A^n$.*

On remarque que le produit des deux foncteurs $\hat{\mathbb{A}}_A^n$ et $\hat{\mathbb{A}}_A^m$ s'identifie canoniquement à $\hat{\mathbb{A}}_A^{n+m}$. On en déduit la proposition suivante :

Proposition 12.3. *Une loi de groupe formelle $\mathcal{G}$ sur A de dimension 1 s'identifie canoniquement à la donnée d'une série formelle $\mathcal{G}(X, Y) \in A[[X, Y]]$ vérifiant les conditions suivantes :*
(i) $\mathcal{G}(X, Y) = X + Y + R$ où R est élément de l'idéal engendré par (X^2, XY, Y^2),

(ii) $\mathcal{G}(X,Y) = \mathcal{G}(Y,X)$,
(iii) $\mathcal{G}(\mathcal{G}(X,Y),Z) = \mathcal{G}(X,\mathcal{G}(Y,Z))$,
(iv) Il existe $i(X)$ *dans* $A[[X]]$ *tel qu'on ait :* $\mathcal{G}(X,i(X)) = 0$.

Un morphisme de lois de groupe formelles $f : \mathcal{G} \to \mathcal{G}'$ s'identifie alors à une série entière $f \in A[[X]]$ telle que l'on ait $f(\mathcal{G}(X,Y)) = \mathcal{G}'(f(X),f(Y))$. Soit F un corps local non archimédien d'anneau d'entiers $\mathcal{O}_F$. On suppose que A objet de $\mathcal{C}$ est muni d'une structure de $\mathcal{O}_F$-algèbre.

Définition 12.4. *Un* $\mathcal{O}_F$*-module formel sur* A *est la donnée d'une loi de groupe* $\mathcal{G}$ *sur* A *ainsi que d'un morphisme d'anneaux* $\mathcal{O}_F \to \mathrm{End}(\mathcal{G})$ *qui à* $a \in \mathcal{O}_F$ *associe* $[a]_{\mathcal{G}}(X) \in A[[X]]$ *série entière satisfaisant :*

$$[a]_{\mathcal{G}}(X) = aX + O(X^2).$$

Soit ϖ une uniformisante de F et $q = p^f$ le cardinal de son corps résiduel. On étudie l'action de ϖ sur un $\mathcal{O}_F$-module formel $\mathcal{G}$ d'anneau de base $\mathcal{O}_F$ où l'on demande de plus à cette action de s'identifier au Frobenius sur $\mathcal{O}_F/\varpi$. La loi est alors dite de Lubin-Tate. Précisément :

Définition 12.5. *Soit* $\mathcal{G}$ *un* $\mathcal{O}_F$*-module formel sur* $\mathcal{O}_F$*. On dit que* $\mathcal{G}$ *est une loi de Lubin-Tate si l'on a*

$$[\varpi]_{\mathcal{G}}(X) = X^q \mod \varpi. \tag{12.1}$$

Le théorème suivant (voir [We]) montre qu'il existe toujours une loi de Lubin-Tate sur un anneau $\mathcal{O}_F$ à uniformisante fixée et que, de plus, une telle loi est unique.

Théorème 12.6. *Soit* $f \in \mathcal{O}_L[X]$ *tel que* $f(X) = \varpi X + O(X^2)$ *et* $f(X) = X^q \mod \varpi$ *alors il existe une unique structure* $\mathcal{G}_f$ *de* $\mathcal{O}_F$*-module formel sur* $\mathcal{O}_F$ *telle que* $[\varpi]_{\mathcal{G}_f}(X) = f(X)$*. De plus si* g *dans* $\mathcal{O}_L[X]$ *vérifie les mêmes conditions, on a :*

$$\mathcal{G}_f \cong \mathcal{G}_g.$$

Remarque 12.7. *Sous les hypothèses du Théorème 12.6, on peut choisir* $f \in \mathcal{O}_L[X]$ *quelconque pourvu qu'on ait* $f(X) = \varpi X + O(X^2)$ *et* $f(X) = X^q \mod \varpi$*. Tout polynôme* f *satisfaisant ces deux mêmes conditions définit la même loi de Lubin-Tate. Dans toute la suite, on peut poser sans perdre en généralité :*

$$f(X) = \varpi X + X^q.$$

Soit $\mathcal{G}$ l'unique loi de Lubin-Tate associée à ϖ sur $\mathcal{O}_F$. On construit une extension de F associée à $\mathcal{G}$, dite extension de Lubin-Tate de F. Pour se faire on fixe une clôture séparable de F noté F^s. On note $\mathfrak{m}$ l'idéal maximal de son anneau d'entiers. Pour tout n dans $\mathbb{N}$ on définit $\mathcal{G}[\varpi^n]$ comme l'ensemble

des éléments x de $\mathfrak{m}$ tels qu'on ait : $[\varpi^n]_{\mathcal{G}}(x) = 0$.

La condition (12.5) de compatibilité au Frobenius permet d'affirmer que $\mathcal{G}[\varpi^n]$ est isomorphe, comme $\mathcal{O}_F/\varpi^n$-module, à $\mathcal{O}_F/\varpi^n$. Cet isomorphisme est compatible aux projections modulo ϖ^m pour m dans $\mathbb{N}$ (voir [We]). On en déduit que la limite projective des $\mathcal{G}[\varpi^n]$ pour n dans $\mathbb{N}$ est un $\mathcal{O}_F$-module libre de rang 1. C'est le ϖ-adique module de Tate. On le note $T_\varpi(\mathcal{G})$.

Soit F_ϖ l'extension de F engendrée par l'union des $\mathcal{G}[\varpi^n]$ pour $n \in \mathbb{N}$. Le groupe de Galois de F_ϖ sur F agit naturellement sur $T_\varpi(\mathcal{G})$ qu'on a vu isomorphe à $\mathcal{O}_F$. On en déduit la représentation suivante :

$$\rho : \mathrm{Gal}(F_\varpi/F) \to \mathcal{O}_F^\times.$$

Définition 12.8. *On appelle caractère de Lubin-Tate, noté χ_{LT} le prolongement de ρ à $\mathrm{Gal}(F^s/F)$. C'est donc un morphisme de groupes :*

$$\chi_{\mathrm{LT}} : \mathrm{Gal}(F^s/F) \to \mathcal{O}_F^\times.$$

Si l'on note F^{ab} l'extension abélienne maximale de F dans F^s et F^{nr} l'extension non ramifiée maximale de F, on a le théorème suivant du à Lubin et Tate (voir [LT]).

Théorème 12.9. *Soit F_ϖ, F^{ab} et F^{nr} comme précédemment, on a :*

$$F^{\mathrm{ab}} = F_\varpi F^{\mathrm{nr}}.$$

12.2 Notations

On fixe une clôture algébrique $\bar{\mathbb{Q}}_p$ de $\mathbb{Q}_p$. Pour toute extension finie F de $\mathbb{Q}_p$ contenue dans $\bar{\mathbb{Q}}_p$, on note $\mathcal{O}_F$ l'anneau des entiers de F et on note $G_F = \mathrm{Gal}(\bar{\mathbb{Q}}_p/F)$ son groupe de Galois absolu.

On fixe K une extension finie de $\mathbb{Q}_p$ et $L \subset \bar{\mathbb{Q}}_p$ un corps de coefficients de dimension finie contenant $\sigma(K)$ pour tout plongement $\sigma : K \hookrightarrow \bar{\mathbb{Q}}_p$. On note K_0 l'extension maximale non ramifiée de $\mathbb{Q}_p$ dans K et $k = \mathbb{F}_q$ (resp. k_L, $\bar{k}$) le corps résiduel de K (resp. L, $\bar{\mathbb{Q}}_p$). On a $q = p^f$ avec $f = [K_0 : \mathbb{Q}_p]$. Soit ϖ_K une uniformisante de $\mathcal{O}_K$ et ϖ_L une uniformisante de $\mathcal{O}_L$. On note φ_q le relèvement de la f-ième puissance du Frobenius sur les anneaux de Witt $W(k_L)$ et $W(\bar{k})$.

Pour tout $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(K, \bar{\mathbb{Q}}_p)$, on fixe une variable formelle t_σ et l'on note $[-]_\sigma$ pour la loi de groupe de Lubin-Tate sur $\sigma(K)$ correspondant à l'uniformisante $\sigma(\varpi_K)$ (voir Théorème 12.6). Pour tout $a \in \mathcal{O}_K$ et $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(K, \bar{\mathbb{Q}}_p)$, cette loi de groupe définit une série entière $[a]_\sigma \in \mathcal{O}_{\sigma(K)}[\![t_\sigma]\!] \subset \mathcal{O}_L[\![t_\sigma]\!]$.

On note $\chi_{\mathrm{LT}} : G_K \to \mathcal{O}_K^\times$ le caractère de Lubin-Tate associé à ϖ_K et $\chi_{\mathrm{LT},\sigma} = \sigma \circ \chi_{\mathrm{LT}} : G_K \to \sigma(\mathcal{O}_K^\times)$ pour σ plongement de $K \hookrightarrow \bar{\mathbb{Q}}_p$. Tous ces

caractères peuvent être vus comme des caractères de G_K à valeurs dans L. Enfin on note

$$\chi_{\mathrm{cyc}} = \prod_{\sigma} \chi_{\mathrm{LT},\sigma} = \mathrm{Nm}_{K/\mathbb{Q}_p} \circ \chi_{\mathrm{LT}}$$

le caractère cyclotomique de G_K.

13 Catégories d'objets semi-linéaires

L'objet de cette section est une adaptation des résultats de Kisin-Ren ([KR]) pour les tours de Lubin-Tate en une variable au cas multivarié. Il s'agit de passer du cas où l'on ne possède qu'une unique filtration sur le corps de base $\mathbb{Q}_p$ au cas où, le corps de base K est une extension finie de $\mathbb{Q}_p$. Ainsi, on obtient une famille de filtrations paramétrées par les plongements du corps de base dans $\bar{\mathbb{Q}}_p$ (voir 13.1 et 13.2). On décrit le lien entre les φ-modules multifiltrés et certains (φ, Γ)-modules (Théorème 13.14).

13.1 Les φ-modules filtrés

Dans ce paragraphe (13.1), K désigne une extension finie de $\mathbf{Q}_p$. Nous donnons ici les définitions des catégories de φ-modules filtrés. Pour une présentation détaillée voir, par exemple [Fo] ou [Be1].

Définition 13.1. *Un* φ-module filtré sur K à coefficients dans L *est un* $L \otimes_{\mathbb{Q}_p} K_0$*-module libre* D *de rang fini muni d'un automorphisme* $\mathrm{id} \otimes \varphi$*-linéaire* $\Phi : D \to D$ *et d'une filtration décroissante exhaustive et séparée* $\mathrm{Fil}^\bullet D_K$ *de* $D_K = D \otimes_{K_0} K$ *par des* $L \otimes_{\mathbb{Q}_p} K$*-sous-modules.*
Un morphisme de $D \to D'$ *de* φ*-modules filtrés est une application* $L \otimes_{\mathbb{Q}_p} K_0$*-linéaire commutant avec l'action des* Φ *et préservant les filtrations.*
La catégorie des φ*-modules filtrés est notée* $\mathrm{Fil}{-}\varphi{-}\mathrm{Mod}_K^L$*. S'il n'y a pas d'ambiguïté sur les rôles des corps* K *et* L*, on note cette catégorie simplement* $\mathrm{Fil}{-}\varphi{-}\mathrm{Mod}$.

Définition 13.2. *Un* φ_q-module filtré sur K à coefficients dans L *est un* L*-espace vectoriel de dimension finie* D *muni d'un automorphisme* $\mathrm{id} \otimes \varphi_q$*-linéaire* $\Phi_q : D \to D$ *et pour tout* $\sigma : K \hookrightarrow L$ *d'une filtration décroissante exhaustive et séparée,* $\mathrm{Fil}_\sigma^\bullet D$ *de* D *par des sous* L*-espaces vectoriels.*
Un morphisme $D \to D'$ *de* φ_q*-modules filtrés est une application linéaire de* D *dans* D' *commutant avec les automorphismes* Φ_q *et préservant les filtrations* $\mathrm{Fil}_\sigma^\bullet$.
La catégorie des φ_q*-modules filtrés est notée* $\mathrm{Fil}{-}\varphi_q{-}\mathrm{Mod}_K^L$*. Si les corps* K *et* L *sont tels qu'il n'y ait pas d'ambiguïté, on les omet dans la notation.*

Dans les catégories $\mathrm{Fil}{-}\varphi{-}\mathrm{Mod}_K^L$ et $\mathrm{Fil}{-}\varphi_q{-}\mathrm{Mod}_K^L$, on peut définir les notions de sommes directes, de produits, de produits tensoriels et de puissance extérieure. Les notions usuelles associées aux pentes ainsi qu'à la semi-stabilité s'étendent également :

Définition 13.3. *(i) Soit* $D \in \mathrm{Fil}-\varphi-\mathrm{Mod}_K^L$ *un objet de rang* 1. *On note* $t_N(D) = \mathrm{val}_p(\det_{K_0} \Phi)$ *la valuation p-adique du déterminant de* Φ *sur* D *vu comme* K_0*-espace vectoriel. Ce déterminant dépend du choix d'une base de* D *sur* K_0 *mais sa valuation est indépendante d'un tel choix. On note de plus :*

$$t_H(D) = \frac{1}{[K:\mathbb{Q}_p]} \sum_{i\in\mathbb{Z}} i \dim_L \Big(\mathrm{gr}_i(D_K) \Big).$$

(ii) Soit $D \in \mathrm{Fil}-\varphi_q-\mathrm{Mod}_K^L$ *un objet de rang* 1, *alors* Φ_q *est simplement la multiplication par un élément* $a \in L^\times$ *et on note* $t_N(D) = \mathrm{val}_p(a)$. *On définit de plus :*

$$t_H(D) = \frac{1}{[K:\mathbb{Q}_p]} \sum_{\sigma} t_{H,\sigma}(D),$$

où $t_{H,\sigma}(D)$ *est l'unique entier tel que*

$$\mathrm{Fil}_\sigma^i D = \begin{cases} D & i \le t_{H,\sigma}(D) \\ 0 & i \ge t_{H,\sigma}(D)+1 \end{cases}$$

(iii) Pour tout φ*-module filtré (ou* φ_q*-module filtré)* D *de rang* d *on note*

$$t_N(D) = t_N(\bigwedge^d D) \text{ et } t_H(D) = t_H(\bigwedge^d D).$$

Le rationnel $\mu(D) = \frac{1}{d}(t_N(D) - t_H(D))$ *est appelé pente de* D.
(iv) Un objet D *de* $\mathrm{Fil}-\varphi-\mathrm{Mod}_K^L$ *(resp. de* $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_K^L$*) est dit semi-stable, si pour tout sous-objet* $D' \subset D$ *stable par* Φ *(resp.* Φ_q*) on a* $\mu(D') \ge \mu(D)$. *L'objet* D *est dit faiblement admissible s'il est semi-stable et de pente* 0.

13.2 Catégories de (φ_q, Γ)-modules en multivariables

On présente, dans ce paragraphe 13.2 une généralisation multivariée de la théorie des (φ, Γ)-modules de Berger ([Be1]). La généralisation au cas de la tour associée à un groupe de Lubin-Tate est due à Kisin et Ren ([KR]) et développée par Berger et Fourquaux ([BF]). La généralisation au cas mutivariée apparaît dans les articles de Berger ([Be2]) et Kedlaya ([Ke]).

On note

$$\mathfrak{S}_L = \mathcal{O}_L[\![(t_\sigma)_\sigma]\!]$$
$$\mathfrak{S}_{\bar{k}} = W(\bar{k})[\varpi_L][\![(t_\sigma)_\sigma]\!].$$

Soit $\mathbb{U} = (\mathrm{Spf}\, \mathfrak{S}_L)^{\mathrm{rig}}$ la fibre générique rigide du spectre formel de $\mathfrak{S}_L$ et

$$\mathcal{O} = \mathcal{O}((t_\sigma)_\sigma) = \Gamma(\mathbb{U}, \mathcal{O}_{\mathbb{U}}) \subset L[\![(t_\sigma)_\sigma]\!]$$

l'anneau des séries de Laurent convergeant sur le polydisque $\mathbb{U}$.
Soit $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(K,\bar{\mathbb{Q}}_p)$, on note $\mathbb{U}_\sigma = (\mathrm{Spf}\,\mathcal{O}_L[\![t_\sigma]\!])^{\mathrm{rig}}$ le disque unité correspondant à la variable t_σ. Son faisceau structural est noté $\mathcal{O}_{\mathbb{U}_\sigma}$. Les sections globales de ce faisceau structural sont notées

$$\mathcal{O}(t_\sigma) = \Gamma(\mathbb{U}_\sigma, \mathcal{O}_{\mathbb{U}_\sigma}).$$

Pour chaque σ on dispose d'un plongement $\iota_\sigma : \mathbb{U}_\sigma \hookrightarrow \mathbb{U}$ donné par $t_{\sigma'} = 0$ pour tout $\sigma' \neq \sigma$.

On note φ_q le relèvement de la q-ième puissance du Frobenius sur $W(\mathbb{F}_q)$ ou $W(\bar{k})$ et l'on étend φ_q aux anneaux $\mathfrak{S}_L, \mathfrak{S}_{\bar{k}}, \mathcal{O}, \mathcal{O}_L(t_\sigma)$ en posant

$$\varphi_q(t_\sigma) = [\varpi]_\sigma(t_\sigma).$$

Si φ_q agit sur un anneau A, pour tout A-module M, on pose $\varphi_q^* M$ le A-module obtenu via la loi $a.m = \varphi_q(a)m$ pour tout $a \in A$ et $m \in M$.

On rappelle que les structures de groupe de Lubin-Tate sont toutes isomorphes (Théorème 12.6), on peut donc sans perdre en généralité en choisir une particulière. On fixe ainsi

$$\varphi_q(t_\sigma) = [\varpi]_\sigma = t_\sigma^q - \sigma(\varpi)t_\sigma.$$

Soit

$$Q_\sigma(t_\sigma) = [\varpi]_\sigma(t_\sigma)/t_\sigma = t_\sigma^{q-1} - \sigma(\varpi) \in \mathcal{O}_L[\![t_\sigma]\!]$$

et $Q = \prod_\sigma Q_\sigma \in \mathfrak{S}_L$ où le produit est pris sur tous les plongements $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(K,\bar{\mathbb{Q}}_p)$. On pose :

$$\lambda_\sigma = \prod\nolimits_{n\geq 0} \varphi_q^n\left(\tfrac{Q_\sigma(t_\sigma)}{Q_\sigma(0)}\right) \in \mathcal{O}(t_\sigma),$$
$$\lambda = \prod\nolimits_\sigma \lambda_\sigma \in \mathcal{O}.$$

Lemme 13.4. *L'ouvert,*

$$U = \bigcup\nolimits_\sigma \{x \in \mathbb{U} \mid \prod\nolimits_{\sigma'\neq\sigma} \lambda_{\sigma'}(x) \neq 0\}$$

est stable sous l'action de φ_q. Le complémentaire fermé de U dans $\mathbb{U}$ est de codimension 2.

Preuve. Le complémentaire de U dans $\mathbb{U}$ s'obtient comme l'union des ensembles $\{(x_{\sigma_1}, x_{\sigma_2})\} \times \prod_{\sigma\neq\sigma_{1,2}} \mathbb{U}_\sigma$, où $x_{\sigma_i} \in \{\lambda_{\sigma_i} = 0\} \subset \mathbb{U}_{\sigma_i}$. □

On note $j : U \hookrightarrow \mathbb{U}$ le plongement ouvert de U dans $\mathbb{U}$. Soit $\Gamma = \mathrm{Gal}(K_{\mathrm{LT}}/K)$ le groupe de Galois de l'extension de Lubin-Tate K_{LT} de K correspondant à l'uniformisante ϖ. Le caractère de Lubin-Tate χ_{LT} identifie Γ avec $\mathcal{O}_K^\times$ (Définition 12.8). On définit une action de Γ sur $\mathcal{O}_L[[t_\sigma]]$ via

$$a \cdot t_\sigma = [a]_\sigma \in \mathcal{O}_L[\![t_\sigma]\!], \quad a \in \Gamma.$$

Cette action s'étend à $\mathfrak{S}_L$ and $\mathcal{O}$.

Définition 13.5. *On note* $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}$ *la catégorie des faisceaux cohérents* $\mathcal{M}$ *sur* $\mathbb{U}$ *vérifiant* $\mathcal{M}=j_*\mathcal{M}_U$ *avec* $\mathcal{M}_U=\mathcal{M}|_U$ *localement libre et où* j_* *désigne le poussé en avant par* $j:U\to\mathbb{U}$. *On demande de plus l'existence d'un isomorphisme*

$$\Phi:(\varphi_q^*\mathcal{M})[1/Q]\longrightarrow\mathcal{M}[1/Q]$$

tel que pour $N\gg 0$ *on ait :*

$$Q^N\mathcal{M}\subset\Phi(\varphi_q^*\mathcal{M})\subset Q^{-N}\mathcal{M}.$$

Enfin, $\mathcal{M}$ *doit être muni d'une action semi-linéaire de* $\Gamma\cong\mathcal{O}_K^\times$ *commutant avec* Φ. *Les morphismes sont les morphismes de faisceaux commutant avec* Φ *et l'action de* Γ.

De même, on peut considérer le cas en une variable, on note $\mathrm{Mod}^{\varphi_q,\Gamma}_{\mathcal{O}_L(t_\sigma)}$ la catégorie obtenue. Par définition, tout objet $\mathcal{M}_\sigma$ de $\mathrm{Mod}^{\varphi_q,\Gamma}_{\mathcal{O}_L(t_\sigma)}$ est un faisceau sur $\mathbb{U}_\sigma$. Soit $D(0,r)$ le disque de centre 0 et de rayon r dans $\mathbb{U}_\sigma$, on note $\mathcal{M}_\sigma(D(0,r))$ la restriction de $\mathcal{M}_\sigma$ à $D(0,r)$. On rappelle ici le lemme 2.1.2 [KR], du originellement à Berger [Be1].

Lemme 13.6. *Soit* $\mathcal{M}_\sigma$ *un objet de* $\mathrm{Mod}^{\varphi_q,\Gamma}_{\mathcal{O}_L(t_\sigma)}$. *Pour tout* $r\in]0,1[$ *et tout* $\gamma\in\Gamma$ *suffisamment proche de* 1, *la série*

$$\log\gamma=\sum_{i=1}^{\infty}(\gamma-1)^i(-1)^{i-1}/i$$

définit un opérateur sur $\mathcal{M}_\sigma(D(0,r))$ *via l'action de* Γ *sur ce module.*
Cet opérateur induit l'existence des applications $\mathbb{Z}_p$*-linéaires entre algèbres de Lie suivantes :*

$$d\Gamma_{\mathcal{O}_L(t_\sigma)}:\mathrm{Lie}\Gamma\to\mathrm{End}_{K_0}\mathcal{O}_L(t_\sigma),$$

et

$$d\Gamma_{\mathcal{M}_\sigma}:\mathrm{Lie}\Gamma\to\mathrm{End}_{K_0}\mathcal{M}_\sigma.$$

Précisément, ces applications s'obtiennent en envoyant $\beta\in\mathrm{Lie}\Gamma$ *sur l'opérateur associé à* $\log(\exp\beta)$. *De plus, l'application* $d\Gamma_{\mathcal{O}_L(t_\sigma)}(\beta)$ *est une dérivation et* $d\Gamma_{\mathcal{M}_\sigma}(\beta)$ *est un opérateur différentielle sur* $d\Gamma_{\mathcal{O}_L(t_\sigma)}(\beta)$. *En d'autres termes, pour* $m\in\mathcal{M}_\sigma$, $f\in\mathcal{O}_L(t_\sigma)$ *et* $\beta\in\mathrm{Lie}\Gamma$ *:*

$$d\Gamma_{\mathcal{M}_\sigma}(\beta)(fm)=d\Gamma_{\mathcal{O}_L(t_\sigma)}(\beta)(f)m+fd\Gamma_{\mathcal{M}_\sigma}(\beta)(m).$$

Définition 13.7. *La catégorie* $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$ *est définie comme la sous catégorie pleine de* $\mathrm{Mod}^{\varphi_q,\Gamma}_{\mathcal{O}_L(t_\sigma)}$ *dont les objets* $\mathcal{M}_\sigma$ *sont tels que l'application* $d\Gamma_{\mathcal{M}_\sigma}$ *est* $\mathcal{O}_L$*-linéaire.*

Définition 13.8. *(i) On définit la catégorie $(\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{an}}_{\mathcal{O}}$ comme la sous catégorie pleine de $(\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}$ dont les objets $\mathcal{M}$ sont tels que $\iota_\sigma^*\mathcal{M} = \mathcal{M}\ \mathrm{mod}(t_{\sigma'})_{\sigma'\neq\sigma}$ est un objet de $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$ pour tout $\sigma\in\mathrm{Hom}(K_0,L)$.*
(ii) On note $(\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{cris}}_{/\mathcal{O}}$ la sous catégorie pleine de $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}$ consistant en les objets dits cristallins $\mathcal{M}$ tels que

$$\dim_L(\mathcal{M}[\tfrac{1}{\lambda}])^\Gamma = \mathrm{rk}\,\mathcal{M}_U.$$

Cette égalité a bien du sens car l'action de L commute avec l'action de Γ. Par suite, $\mathcal{M}[1/\lambda]^\Gamma$ est un L-espace vectoriel.

Remarque 13.9. *La terminologie "cristallin" introduite dans la définition 13.8 est motivée par le cas univarié dans lequel Kisin et Ren ont établi que les représentations galoisiennes associées à ces modules étaient cristallines au sens de Fontaine ([KR]). D'après le Corollaire 7.2 de [Be1],on a toujours :*

$$\dim_L(\mathcal{M}[\tfrac{1}{\lambda}])^\Gamma \leq \mathrm{rk}\,\mathcal{M}_U.$$

Ainsi, un (φ_q,Γ)-module $\mathcal{M}$ est cristallin si et seulement si l'espace invariant par Γ dans $\mathcal{M}[1/\lambda]$ est aussi grand que possible.
Berger donne une définition moins naïve du caractère cristallin multivarié (Définition 7.3 [Be2] qui lui permet d'obtenir l'équivalence entre les catégories de (φ_q,Γ)-modules cristallins et les φ_q-modules avec h filtrations (Théorème 7.9 [Be2]).

Remarque 13.10. *On a $(\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{cris}}_{/\mathcal{O}} \subset (\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{an}}_{\mathcal{O}}$. En effet, si $\mathcal{M}$ est cristallin,*

$$\mathcal{M}[1/\lambda]^\Gamma\otimes_L\mathcal{O}(t_\sigma)[1/\lambda_\sigma]\cong\iota_\sigma^*(\mathcal{M})[1/\lambda_\sigma].$$

En particulier, l'action de Γ sur $\iota_\sigma^*(\mathcal{M})[1/\lambda_\sigma]$ est isomorphe à l'action de Γ sur $\mathcal{O}(t_\sigma)[1/\lambda_\sigma]^d$. On en déduit que l'action de $\mathrm{Lie}\,\Gamma$ est $\mathcal{O}_F$-linéaire.

Exemple 13.11. *Soit $\delta : K^\times\to L^\times$ un caractère continu. On peut alors définir $D(\delta)$ comme le $\mathcal{O}((t_\sigma)_\sigma)$-module libre de rang 1 et de générateur e tel que $\varphi(e)=\delta(\varpi_K)e$ et $\gamma\cdot e=\delta(\gamma)e$. Ce module est alors cristallin si et seulement si δ est algébrique en d'autres termes, si $\delta|_{\mathcal{O}_K^\times}$ est de la forme*

$$z\longmapsto\prod_{\sigma:K\hookrightarrow L}\sigma(z)^{n_\sigma}$$

avec $n_\sigma\in\mathbb{Z}$ pour tout σ plongement de K dans L.

Définition 13.12. *Soit $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_L$ la catégorie des L-espaces vectoriels D de dimension finie munis d'un isomorphisme φ_q-linéaire et d'une filtration décroissante exhaustive et séparée sur D, indexée par $\mathbb{Z}$, de L-espaces vectoriels. Les morphismes sont les morphismes de L-espaces vectoriels commutant avec les φ_q-isomorphisme et respectant les filtrations.*

Le lemme suivant (voir Lemma 2.2.2 [Be1], Prop. 2.2.6 [KR]) est l'argument clé prouvant l'équivalence de catégories entre $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$ et $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_L$.

Lemme 13.13. *Soit $\mathcal{M}_\sigma$ un objet de $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$. Il existe une unique section L-linéaire $\xi_\sigma : \mathcal{M}_\sigma/t_\sigma\mathcal{M}_\sigma \to \mathcal{M}_\sigma[1/\lambda_\sigma]$ telle que les éléments $\xi_\sigma(\mathcal{M}_\sigma/t_\sigma\mathcal{M}_\sigma)$ soient Γ-invariant. On a de plus :*

(i) l'application ξ_σ est φ_q-equivariante.

(ii) L'application ξ_σ induit un isomorphisme :

$$\mathcal{M}_\sigma/t_\sigma\mathcal{M}_\sigma \otimes_L \mathcal{O}_L(t_\sigma)[1/\lambda_\sigma] \to \mathcal{M}_\sigma[1/\lambda_\sigma].$$

(iii) Si $v_m \in \overline{\mathbb{Q}}_p$ est tel que $[\varpi_K^m]_\sigma(v_m) = 0$, ξ_σ induit un isomorphisme :

$$\mathcal{M}_\sigma/t_\sigma\mathcal{M}_\sigma \otimes_L L(v_m) \to \varphi_q^*(\mathcal{M}_\sigma)/Q_\sigma\varphi_q^*(\mathcal{M}_\sigma).$$

Pour tout σ fixé, il existe une équivalence de catégories entre $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$ et $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_L$ donnée par :

$$\mathbf{D}_\sigma : \mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)} \to \mathrm{Fil}-\varphi_q-\mathrm{Mod}_L.$$

On rappelle la construction de Kisin-Ren de $\mathbf{D}_\sigma$ (Proposition 2.2.6 [KR]).
Soit $\mathcal{M}_\sigma$ un objet de $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$. Pour $i \in \mathbb{Z}$, soit $\mathrm{Fil}^i\varphi_q^*\mathcal{M}_\sigma$ la préimage de $Q_\sigma^i\mathcal{M}_\sigma$ par Φ_σ.
Comme l'action de Γ commute avec Φ_σ et que Q_σ divise $[\gamma]_\sigma(Q_\sigma)$, cette filtration est stable par Γ. Pour $\mathbf{D}_\sigma(\mathcal{M}_\sigma) = \mathcal{M}_\sigma/t_\sigma\mathcal{M}_\sigma$, par le lemme 13.13, ξ_σ induit un isomorphisme :

$$\mathbf{D}_\sigma(\mathcal{M}_\sigma) \otimes_L L(v_m) \to \varphi_q^*(\mathcal{M}_\sigma)/Q_\sigma\varphi_q^*(\mathcal{M}_\sigma).$$

Le tiré en arrière de $\mathrm{Fil}^i\varphi_q^*\mathcal{M}_\sigma$ dans $\mathbf{D}_\sigma(\mathcal{M}_\sigma) \otimes_L L(v_m)$ est Γ-stable et induit donc une filtration sur $\mathbf{D}_\sigma(\mathcal{M}_\sigma)$.

Théorème 13.14. *Il existe un foncteur naturel :*

$$\mathbf{D} : (\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{cris}}_{\mathcal{O}} \to \mathrm{Fil}-\varphi_q-\mathrm{Mod}^K_L.$$

Preuve. Soit $\mathcal{M} \in (\varphi_q,\Gamma)-\mathrm{Mod}^{\mathrm{cris}}_{\mathcal{O}}$ de rang d on définit $\mathbf{D}(\mathcal{M}) = (\mathcal{M}[1/\lambda])^\Gamma$. C'est un espace vectoriel sur L de dimension d équipé d'un isomorphisme induit par Φ sur $\mathcal{M}$, φ_q-linéaire. On pose de plus, $\mathcal{M}_\sigma = \iota_\sigma^*(\mathcal{M}|_{U_\sigma})$. Comme $\mathcal{M}|_{U_\sigma}$ est libre de rang d il en va de même pour $\mathcal{M}_\sigma$. Ainsi $\mathcal{M}_\sigma$ objet de $\mathrm{Mod}^{\varphi_q,\Gamma}_{\mathcal{O}_L(t_\sigma)}$. L'isomorphisme canonique

$$\mathbf{D}(\mathcal{M}) \otimes_L \mathcal{O}[1/\lambda] \longrightarrow \mathcal{M}[1/\lambda]$$

induit un isomorphisme $\mathbf{D}(\mathcal{M}) \to \mathcal{M}/(t_\sigma, \sigma) \cong \mathcal{M}_\sigma/(t_\sigma)$ qui commute avec l'action de Φ. On en déduit aussi que

$$\mathcal{M}_\sigma/(t_\sigma) \otimes_L \mathcal{O}(t_\sigma) \longrightarrow \mathcal{M}_\sigma[1/\lambda_\sigma]$$

est un isomorphisme. Par suite, $\mathcal{M}_\sigma$ est un objet de $\mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$. On peut lui appliquer le foncteur $\mathbf{D}_\sigma$ et l'on obtient un isomorphisme Φ-équivariant : $D \cong \mathbf{D}_\sigma(\mathcal{M}_\sigma)$. En tirant en arrière la filtration $\mathrm{Fil}^\bullet_\sigma$ sur $\mathbf{D}_\sigma(\mathcal{M}_\sigma)$ le long de cet isomorphisme, on équipe $\mathbf{D}(\mathcal{M})$ d'une structure qui en fait un objet de $\mathrm{Fil}{-}\varphi_q{-}\mathrm{Mod}^K_L$. □

Proposition 13.15. *Il existe un foncteur naturel :*

$$\mathbf{M} : \mathrm{Fil}{-}\varphi_q{-}\mathrm{Mod}^K_L \to (\varphi_q, \Gamma){-}\mathrm{Mod}_{\mathcal{O}}.$$

Preuve. Soit $D \in \mathrm{Fil}{-}\varphi_q{-}\mathrm{Mod}^K_L$ et soit σ fixé. On note D_σ l'objet de cette même catégorie possédant la structure de D comme φ_q-module et la même filtration associée à σ, $\mathrm{Fil}^\bullet_\sigma$. On suppose de plus que pour $\sigma' \neq \sigma$ tout autre plongement la filtration associée $\mathrm{Fil}^\bullet_{\sigma'}$ est triviale. On en déduit qu'il existe à isomorphisme près un unique objet $\mathcal{M}_\sigma \in \mathrm{Mod}^{\varphi_q,\Gamma,\mathrm{an}}_{\mathcal{O}_L(t_\sigma)}$ tel que $\mathbf{D}_\sigma(\mathcal{M}_\sigma) = D_\sigma$. Via le morphisme ξ_σ construit dans le lemme 13.13 on peut voir $\mathcal{M}_\sigma$ comme un sous module de $D \otimes_L \mathcal{O}_\sigma[1/\lambda_\sigma]$. On note $\mathcal{M}'_\sigma$ le tiré en arrière de $\mathcal{M}_\sigma$ le long de $U_\sigma \to \mathbb{U}_\sigma$. Pour $n = 1$ on obtient ainsi un objet de $(\varphi_q, \Gamma){-}\mathrm{Mod}_{\mathcal{O}}$. Pour $n \neq 1$ et $\sigma \neq \sigma'$ les restrictions $\mathcal{M}'_\sigma|_{U_\sigma \cap U_{\sigma'}}$ et $\mathcal{M}'_{\sigma'}|_{U_\sigma \cap U_{\sigma'}}$ coïncident avec $D \otimes_L \mathcal{O}[1/\lambda]$. On peut donc recoller $\mathcal{M}'_\sigma$ pour tout σ et l'on obtient un module $\mathcal{M}'$ sur U muni d'une action de Γ et d'un isomorphisme φ_q-linéaire commutant avec cette action.

Comme le fermé complémentaire de U est de codimension 2 (Lemme 13.4) le faisceau $\mathcal{M} = j_*\mathcal{M}'$ est cohérent et fait de $\mathcal{M}$ un objet de $(\varphi_q, \Gamma){-}\mathrm{Mod}_{\mathcal{O}}$. □

14 Objets admissibles

L'objet de cette section §14 est de définir l'analogue multivarié des φ_q-modules de Hodge-Pink de Genestier-Lafforgue ([GL]).
Dans [GL], à un objet de Fil-φ_q-Mod_L est associé un φ_q-module de Hodge-Pink. La faible admissibilité de l'objet D de Fil-φ_q-Mod_L garantie la convergence d'une suite de $\mathcal{O}_L$ réseaux dans D. La convergence est contrôlé grâce à une famille bornée d'objets, dits pseudo-iso-$\mathfrak{S}$-modules. On détaille les définitions de ces objets dans le cas multivarié (14.1), puis certaines difficultés nouvelles qui apparaissent dans notre situation généralisée.

14.1 Modules de Hodge-Pink

Soit $\hat{\mathfrak{S}}_{Q_\sigma}$ (respectivement $\hat{\mathfrak{S}}_{\bar{k},Q_\sigma}$) la complétion de $\mathcal{O}_L[\![t_\sigma]\!][1/p]$ (respectivement $W(\bar{k})[\varpi_L][[t_\sigma]][1/p]$) selon l'idéal engendré par Q_σ.

Définition 14.1. *Soit D un L (respectivement un $W(\bar{k})[1/p]$) espace vectoriel. Une* σ-structure de Hodge-Pink *sur D est un $\hat{\mathfrak{S}}_{Q_\sigma}$-réseau (respectivement un $\hat{\mathfrak{S}}_{\bar{k},Q_\sigma}$-réseau) $V_{D,\sigma} \subset \varphi_q^*(D) \otimes_L \hat{\mathfrak{S}}_{Q_\sigma}[1/Q_\sigma]$ (respectivement $V_{D,\sigma} \subset \varphi_q^*(D) \otimes_{W(\bar{k})[\varpi_L][1/p]} \hat{\mathfrak{S}}_{\bar{k},Q_\sigma}[1/Q_\sigma]$) .*
Un φ_q-module de Hodge-Pink *sur L (respectivement $W(\bar{k})[\varpi_L][1/p]$) est un L-espace vectoriel D (respectivement espace vectoriel sur $W(\bar{k})[\varpi_L][1/p]$) muni d'un φ_q-isomorphisme Φ_D sur D et d'une σ-structure de Hodge-Pink pour tout $\sigma \in \mathrm{Hom}_{\mathbb{Q}_p}(K, \bar{\mathbb{Q}}_p)$.*
Un morphisme $f : (D, \Phi, (V_\sigma)_\sigma) \to (D', \Phi', (V'_\sigma)_\sigma)$ de φ_q-module de Hodge-Pink est un morphisme $f : D \to D'$ de L-espaces vectoriels (respectivement un morphisme de $W(\bar{k})[\varpi_L][1/p]$-espaces vectoriels) tel que

$$f \circ \Phi = \Phi' \circ f \text{ et } f(V_\sigma) \subset V'_\sigma$$

pour tout σ. La catégorie des φ_q-modules de Hodge Pink sur L est notée $\mathrm{HP} - \mathrm{Mod}_{\varphi_q}$.

La catégorie $\mathrm{HP} - \mathrm{Mod}_{\varphi_q}$ est munie des notions usuelles de sommes directes, produits, produits tensoriels et puissances extérieures. On peut de plus y définir des notions de pentes et de semi-stabilité :

Définition 14.2. *(i) Soit $D \in \mathrm{HP} - \mathrm{Mod}_{\varphi_q}$ un objet de rang 1. Alors l'isomorphisme Φ_D s'obtient comme produit par un certain $a \in L^\times$ on définit alors $t_N(D)$ par $t_N(D) = \mathrm{val}_p(a)$. Puis le rationnel $t_H(D)$ par :*

$$t_H(D) = \frac{1}{[K : \mathbb{Q}_p]} \sum_\sigma t_{H,\sigma}(D),$$

où $t_{H,\sigma}(D)$ est l'unique entier tel que

$$V_\sigma = Q_\sigma^{-t_{H,\sigma}(D)}\big(D \otimes_L \hat{\mathfrak{S}}_{Q_\sigma}\big).$$

(ii) Pour D quelconque de rang d, on définit $t_N(D)$ et $t_H(D)$ via les identités :

$$t_N(D) = t_N(\bigwedge^d D) \text{ et } t_H(D) = t_H(\bigwedge^d D).$$

On pose alors $\mu(D) = \frac{1}{d}(t_N(D) - t_H(D))$ qu'on appelle pente de D.
(iii) Un objet D est dit semi-stable, si pour tout Φ_D-sous objet stable $D' \subset D$ on a $\mu(D') \geq \mu(D)$. L'objet D est dit faiblement admissible s'il est semi-stable de pente égale à 0.

Notation 14.3. *Soit $D \in \mathrm{HP} - \mathrm{Mod}_{\varphi_q}$, on note $U_\sigma = D \otimes_L \hat{\mathfrak{S}}_{Q_\sigma}$ le réseau naturel de $D \otimes_L \hat{\mathfrak{S}}_{Q_\sigma}[1/Q_\sigma]$.*

Définition 14.4. *Soit X un espace analytique rigide et $\mathfrak{X}$ un schéma formel dont il est issu. Soit $\mathcal{L}$ un faisceau sur X. On appelle modèle de $\mathcal{L}$ un faisceau sur $\mathfrak{X}$ dont le rigidifié s'identifie à $\mathcal{L}$.*

Définition 14.5. *Soit $\mathcal{M}$ un objet de la catégorie $(\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}^{\mathrm{an}}$ et $\mathfrak{N}$ un modèle de $\mathcal{M}$. Comme $\mathcal{M}$ est cohérent et défini sur le rigidifié d'un schéma formel affine on peut identifier $\mathfrak{N}$ à un $\mathcal{O}_L[[(t_\sigma)_\sigma]]$-module de rang fini. Dans la suite on note $\mathfrak{N}_\sigma$ le tiré en arrière de $\mathfrak{N}$ selon ι_σ.*
On définit $V_{\mathbf{D}(\mathcal{M}),\sigma}$ la σ-structure de Hodge-Pink associée à σ sur $D=\mathbf{D}(\mathcal{M})$ par:

$$V_{\mathbf{D}(\mathcal{M}),\sigma}=\varphi_q^*\xi_\sigma^{-1}((\Phi_{\mathfrak{N}_\sigma}\otimes 1)^{-1}(\mathfrak{N}_\sigma\otimes_{\mathcal{O}_L[[t_\sigma]]}\hat{\mathfrak{S}}_{Q_\sigma}))$$

Ainsi défini, $(D,\Phi_D,(V_{\mathbf{D}(\mathcal{M}),\sigma})_\sigma)$ est un φ_q-module de Hodge-Pink.
Cette construction induit un foncteur $\mathbf{D}'$ entre la catégorie $(\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}^{\mathrm{an}}$ et la catégorie des φ_q-modules de Hodge-Pink :

$$\mathbf{D}':(\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}^{\mathrm{an}}\to \mathrm{HP}-\mathrm{Mod}_{\varphi_q}.$$

Remarque 14.6. *Suivant les idées de [GL] §1, on construit un foncteur $\boldsymbol{V}$ de la catégorie des φ_q-modules de Hodge-Pink, $\mathrm{HP}-\mathrm{Mod}_{\varphi_q}$ vers la catégorie des φ_q-modules filtrés, $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_K^L$:*

$$\boldsymbol{V}:\mathrm{HP}-\mathrm{Mod}_{\varphi_q}\to \mathrm{Fil}-\varphi_q-\mathrm{Mod}_K^L.$$

$\boldsymbol{V}$ est défini via:

$$\Phi_D^{-1}(\mathrm{Fil}_\sigma^i(D))=(Q_\sigma^iV_{D,\sigma}\cap U_{D,\sigma})/(Q_\sigma^iV_{D,\sigma}\cap Q_\sigma U_{D,\sigma}).$$

Soit D un objet de $\mathrm{HP}-\mathrm{Mod}_{\varphi_q}$, cette construction induit l'égalité suivante :

$$t_H(\boldsymbol{V}(D),\sigma)=t_H(D,\sigma).$$

En d'autres termes, $\boldsymbol{V}$ préserve la faible admissibilité.

D'après [KR] 2.2.2, la filtration $\mathrm{Fil}_\sigma^i\mathbf{D}(\mathcal{M})$ obtenue par le foncteur $\mathbf{D}$ est la même que celle qui se déduit des applications successives de $\mathbf{D}'$et $\boldsymbol{V}$. On a le diagramme commutatif suivant :

$$\begin{array}{ccc}(\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}^{\mathrm{an}} & \xrightarrow{\mathbf{D}'} & \mathrm{HP}-\mathrm{Mod}_{\varphi_q}\\ \downarrow{\scriptstyle\mathbf{D}} & \swarrow{\scriptstyle\boldsymbol{V}} & \\ \mathrm{Fil}-\varphi_q-\mathrm{Mod}_L^K & & \end{array}\qquad(14.1)$$

Soit $(D,\Phi,\mathrm{Fil}_\sigma^\bullet)$ un objet de $\mathrm{Fil}-\varphi_q-\mathrm{Mod}_K^L$. Pour tout σ, [GL] lemma 1.3 définit une section du foncteur $\boldsymbol{V}$. Cette section préserve la faible admissibilité ([GL] lemma 1.4), On peut associer à la filtration $\mathrm{Fil}_\sigma^\bullet$ un $\hat{\mathfrak{S}}_{Q_\sigma}$-réseau $V_{D,\sigma}\subset D\otimes_L\hat{\mathfrak{S}}_{Q_\sigma}[1/Q_\sigma]$. Par suite on peut définir $\boldsymbol{V}'$ section du foncteur $\boldsymbol{V}$. Cette section n'est pas un foncteur inverse : on a bien $\boldsymbol{V}\circ\boldsymbol{V}'=\mathrm{id}$ mais pas $\boldsymbol{V}'\circ\boldsymbol{V}\neq\mathrm{id}$, $\boldsymbol{V}$ n'étant pas essentiellement injectif.

Définition 14.7. *On note* $\mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ *la catégorie des pseudo-iso-*$\mathfrak{S}_L[1/p]$*-modules* $\mathfrak{N}$*, formée des* $\mathfrak{S}_L[1/p]$*-modules* $\mathfrak{N}$ *de rang fini, muni d'un isomorphisme*

$$\Phi : (\varphi_q^*\mathfrak{N})[1/Q] \to \mathfrak{N}[1/Q]$$

et d'une action semi-linéaire de Γ *commutant avec* Φ*.*
On suppose de plus que $\mathfrak{N}$ *est sans torsion et que pour* $s \leq t$ *in* $\mathbb{Z}$ *dépendant uniquement de* $\mathfrak{N}$*, on a pour tout* $\mathfrak{S}_L$*-submodule* $\mathfrak{M} \subset \mathfrak{N}$ *satisfaisant* $\mathfrak{M}[1/p] = \mathfrak{N}$ *une constante* C *dépendant de* $\mathfrak{M}$ *telle que pour tout* $n \in \mathbb{N}$ *on ait :*

$$\begin{aligned}\Phi \circ \varphi_q^*\Phi \circ \cdots \circ (\varphi_q^{n-1})^*\Phi &\in p^{-C}Q^s\varphi_q(Q)^s \ldots \varphi_q^{n-1}(Q)^s \,\mathrm{Hom}((\varphi_q^n)^*\mathfrak{M}, \mathfrak{M}),\\ \left(\Phi \circ \varphi_q^*\Phi \circ \cdots \circ (\varphi_q^{n-1})^*\Phi\right)^{-1} &\in p^{-C}Q^{-t}\varphi_q(Q)^{-t} \ldots \varphi_q^{n-1}(Q)^{-t} \,\mathrm{Hom}(\mathfrak{M}, (\varphi_q^n)^*\mathfrak{M}).\end{aligned} \tag{14.2}$$

Soit une $\mathbb{Z}_p$-algèbre R locale complète et noethérienne de corps résiduel fini et un $R[1/p]$-module $\mathfrak{N}$ de type fini. On définit un faisceau cohérent $\mathcal{N}$ sur la fibre générique de l'espace rigidifié $(\mathrm{Spf}\, R)^{\mathrm{rig}}$ de la manière suivante : Soit $\mathfrak{M} \subset \mathfrak{N}$ un sous-R-module quelconque tel que $\mathfrak{N} = \mathfrak{M}[1/p]$. Soit $\mathcal{N}$ la fibre générique du rigidifié de $\mathfrak{M}$. On vérifie que $\mathcal{N}$ est indépendant du choix d'un modèle intégral $\mathfrak{M}$ de $\mathfrak{N}$, on dira que $\mathcal{N}$ est la fibre rigide de $\mathfrak{N}$.

On peut remarquer que $\mathcal{N}$ fibre rigide d'un objet $\mathfrak{N}$ de $\mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ n'est pas nécessairement objet de $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}$, en effet rien n'assure que la restriction $\mathcal{N}|_U$ soit libre ni non plus que l'on ait $j_*\mathcal{N}_U = \mathcal{N}$. C'est bien le cas pourtant si l'on suppose $\mathfrak{N}$ libre comme $\mathfrak{S}[1/p]$ module. Pour $n = 1$ le travail de Genestier-Lafforgue (voir [GL]) montre qu'il suffit de se restreindre à de tels modules (libres) pour définir correctement l'admissibilité. Dans le cas général nous ne savons pas si une telle restriction permet de tenir compte de tous les objets admissibles. On ne sait pas si tout objet de $\mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ peut être considéré comme libre sur $\mathfrak{S}[1/p]$. La catégorie $\mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ va servir dans la suite de "modèle entier" pour les catégories $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}$ et $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}^{\mathrm{cris}}$.

Définition 14.8. *Un objet* $\mathcal{M} \in (\varphi_q,\Gamma)-\mathrm{Mod}_{\mathcal{O}}^{\mathrm{an}}$ *est dit admissible s'il existe* $\mathfrak{N} \in \mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ *tel que* $\mathcal{M}$ *soit la fibre rigide de* $\mathfrak{N}$*, son action par* Γ *et l'existence de* Φ *se déduisant alors de l'action de* Γ *et de l'existence de* Φ *sur* $\mathfrak{N}$*. On dit alors que* $\mathfrak{N}$ *est un modèle de* $\mathcal{M}$*.*

Proposition 14.9. *Soit* $\mathcal{M}$ *un objet admissible de* $(\varphi_q,\Gamma)-\mathrm{Mod}_{/\mathcal{O}}^{\mathrm{cris}}$ *alors* $\mathcal{M}$ *est libre. De plus il existe un modèle* $\mathfrak{N} \in \mathrm{PIMod}_{/\mathfrak{S}}^{\varphi_q,\Gamma}$ *de* $\mathcal{M}$ *qui est localement libre.*

Preuve. Soit $X \subset \mathbb{U}$ le sous-ensemble des $x \in \mathbb{U}$ tel que l'on ait $\dim_{k(x)} \mathcal{M} \otimes k(x) > d$, où d désigne le rang générique de $\mathcal{M}$. Alors X est fermé de codimension au moins 2 et stable par φ_q. Soit $\mathfrak{N}$ un modèle $\mathcal{M}$ et soit R un quotient de $\mathfrak{S}$ tel qu'on ait pour tout $y \in \mathrm{Spec}\, R[1/p]$ l'inégalité :

$\dim_{k(y)} \mathfrak{N} \otimes k(y) > d$. L'ensemble X s'identifie alors a la fibre rigide de $\operatorname{Spf} R$ et ainsi n'a qu'un nombre fini de composantes irréductibles. Donc l'ensemble X est soit vide soit muni d'un nombre infini de composantes irréductibles. Ainsi, X est vide et par suite $\mathfrak{N}$ est localement libre. □

Corollaire 14.10. *Soit $\mathcal{M} \in (\varphi_q, \Gamma)-\mathrm{Mod}^{\mathrm{cris}}_{/\mathcal{O}}$ un objet admissible et soit $\mathfrak{N} \in \mathrm{PIMod}^{\varphi_q,\Gamma}_{/\mathfrak{S}}$ un modèle pour $\mathcal{M}$. Alors on a $\mathfrak{N}$ localement libre.*

Preuve. Il existe une bijection entre les points fermés de $\operatorname{Spec} \mathfrak{S}[1/p]$ et les points de l'espace rigidifié $\mathbb{U} = (\operatorname{Spf} \mathfrak{S})^{\mathrm{rig}}$. Soit un tel point $x \in \operatorname{Spec} \mathfrak{S}[1/p]$ on note $\tilde{x}$ le point associé dans $\mathbb{U}$. Par définition de $\mathfrak{N}$ comme modèle de $\mathcal{M}$, il vient $\mathfrak{N} \otimes k(x) = \mathcal{M} \otimes k(\tilde{x})$. On en déduit, en appliquant 14.9 que $\dim_{k(x)} \mathfrak{N} \otimes k(x)$ est constant sur $\operatorname{Spec} \mathfrak{S}[1/p]$. Ce schéma étant réduit, on en déduit que $\mathfrak{N}$ est localement libre. □

Remarque 14.11. *Dans le corollaire 14.10, on ne peut pas garantir que $\mathfrak{N}$ soit libre comme $\mathfrak{S}[1/p]$-module, la question reste ouverte.*

Par définition (14.7), les pseudo-iso-$\mathfrak{S}$ modules se caractérisent par le fait que tout itéré de leur Frobenius reste borné. C'est cette propriété qui caractérise la faible admissibilité des φ_q-modules filtrés.

Précisons la stratégie de Genestier et Lafforgue ([GL]) dans le cas de la tour cyclotomique (en une variable t) et lorsque L est totalement ramifié sur $\mathbb{Q}_p$. Genestier et Lafforgue prouvent l'équivalence entre admissibilité (définie dans 14.8) et faible admissibilité.

A chaque φ-module de Hodge-Pink irréductible et défini sur $W(\bar{k})[1/p]$ associé à un φ-module filtré D, Genestier et Lafforgue associent une suite de modules sur $\mathfrak{S}$ inclus dans $D \otimes \mathfrak{S}[1/p]$. La réduction de cette suite de $\mathfrak{S}$-modules modulo t définit une suite de réseaux sur $\mathcal{O}_L$ inclus dans D. La faiblement admissibilité du φ-module filtré se traduit par le fait que la suite de réseaux restent bornée. Précisément, si Δ est le réseau initial et $(\gamma_n(\Delta))_{n\in\mathbb{N}}$ la suite de réseau associé au φ-module filtré, la faible admissibilité implique qu'il existe un C entier naturel tel que pour tout $n \in \mathbb{N}$ on ait :

$$p^C \Delta \subset \gamma_n(\Delta) \subset p^{-C} \Delta. \tag{14.3}$$

Par ailleurs, Genestier et Lafforgue montrent qu'une telle propriété (14.3) de la suite $(\gamma_n(\Delta))_{n\in\mathbb{N}}$ est équivalente à l'admissibilité au sens de 14.8. Ils en déduisent l'équivalence entre admissibilité et la faible admissibilité.

On voit ainsi l'importance de définir les structures de Hodge-Pink et les pseudo-iso-$\mathfrak{S}$ module, ces derniers traduisent en terme de lieu d'évolution des itérés du Frobenius la faible admissibilité et donc par là l'admissibilité

des représentations cristallines. Cependant lorsque l'on remplace tour cyclotomique et tour de Lubin-Tate, il est difficile de contrôler la convergence des suites de réseaux.

References

[Be1] L. Berger, *Equations différentielles p-adiques et (φ, N)-modules filtrés.* Astérisque **319**, 2008, 13–38.

[Be2] L. Berger, *Multivariable Lubin-Tate (φ, Γ)-modules and filtrered φ-modules.* ArXiv: 1211.4431, 2013.

[BF] L. Berger, L. Fourquaux, *Iwasawa theory and F-analytic Lubin-Tate (φ, Γ)-modules.* HAL- 01255343, 2015.

[CF] P. Colmez, J.-M. Fontaine, *Construction des représentations p-adiques semi-stables.* Invent. Math. **140**, 2000, 1–43.

[Fo] J.-M. Fontaine, *Représentations p adiques des corps locaux. 1.* Dans The Grothendieck Festschrift, Vol. II. Progr. Math. **87**, 1990, 249–209.

[GL] A. Genestier, V. Lafforgue, *Structures de Hodge-Pink pour les $\varphi/\mathfrak{S}$-modules de Breuil et Kisin.* Compositio Mathematica **148**, 2012, 751–789.

[HH] U. Hartl, E. Hellmann, *The universal family of semi-stable p-adic Galois representations.* ArXiv 1312. 6371, 2013.

[Ke] K.S. Kedlaya, *Some slope theory for multivariate Robba Rings.* arXiv:1311.7468.

[Ki] M. Kisin, *Crystalline representations and F-crystals.* Progress in Mathematics **253**, 2006, 459–496.

[KR] M. Kisin, W. Ren, *Galois representations and Lubin-Tate groups.* Documenta Mathematica **14**, 2009, 441–461.

[LT] J. Lubin, J. Tate, *Formal complex multiplication in local fields.* Annals of Mathematics. Second Series 81, 1965, 380-387.

[We] J. Weinstein : *The Geometry of Lubin-Tate spaces.* Lecture 1, MSRI, 2014.

Part III

Schémas numériques d'ordre 2 en temps pour les équations de désorption 1D d'un gaz de schiste

15 Introduction

Ce rapport contient des éléments de réponse concernant le problème posé par l'Institut Français du Pétrole et des Energies Nouvelles (IFPEN) lors de la treizième Semaine d'Etude Maths-Entreprise (SEME). Il a été effectué en collaboration avec Victor Vilaça Da Rocha, Roberta Tittarelli, Richard Sambilason Rafefimanana, Victor Michel-Dansac et Benjamin Couéraud.

Les SEME sont une initiative de l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société. Elles visent "à créer des échanges entre les milieux industriels et le monde académique par le biais d'une semaine de travail sur des problèmes posés par des industriels et nécessitant des approches mathématiques et informatiques innovantes."

Le problème concernait la résolution numérique d'un système d'équations modélisant la désorption d'un gaz de schiste, en une dimension. L'extraction de gaz de schiste, méthode critiquée, mérite plus qu'une autre une juste modélisation de ces effets. Le présent travail tente d'éclaircir la façon dont on modélise sa désorption i.e. la chute de pression qu'elle provoque . Le système d'équation modélisant cette variation de la pression et du volume du gaz dans la faille nous a été soumis par l'IFPEN. Nous modélisons -le plus simplement possible- ces équations afin de disposer d'une évaluation prédictive et concrète des variables du problème, la pression, le volume, sous contraintes. La fracture dans la roche où se trouve le gaz est modélisé par un segment de longueur fixée. On modélise, à partir du début du pompage, la pression en tout temps et en tout points de la faille.

Une telle modélisation peut s'avérer cruciale, par exemple, pour la sécurité des sols au voisinage d'une faille utile à l'exploitation du schiste. Une baisse violente mal contrôlée, en un point donné de la pression du gaz peut occasionner une fragilité des sols. Nous n'avons pas les connaissances requises pour dire si tel est le cas. Les schémas eux-mêmes, sont, par leur simplicité, sujets à débat.

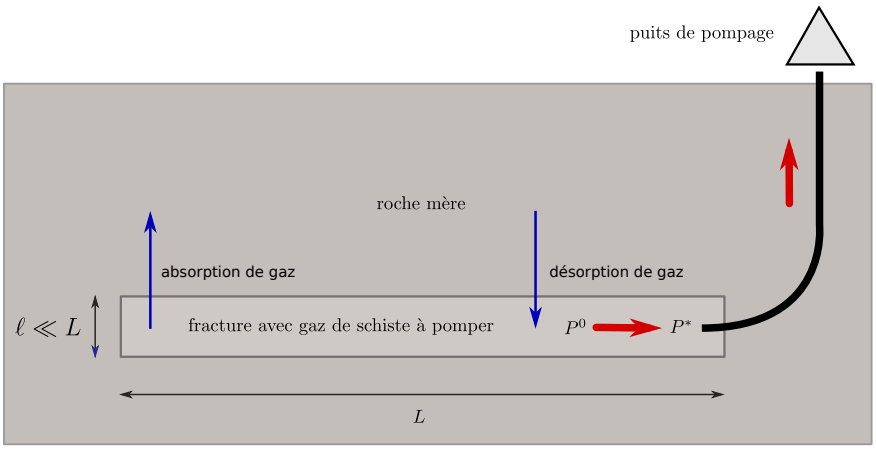
Après une présentation du problème, nous exposons nos résultats; le premier schéma numérique donne des résultats encourageants. Par la suite, plusieurs possibilités sont évoquées pour monter en ordre à partir de ce schéma numérique.

Une fois posées les données du problème (§16), nous donnons la discrétisation utilisée pour la partie spatiale (§17). Puis nous explicitons le schéma du premier ordre en temps (§18). Nous testons alors plusieurs hypothèses de modélisation. La première (18.1) est un schéma explicite en espace. La seconde (18.2) est un schéma implicite dans lequel il n'existe pas de couplage

entre les valeurs de volume et pression. Enfin la dernière (18.3) reprend un schéma implicite en espace du premier ordre en lui associant à chaque pas de discrétisation, un couplage volume/pression. Nous analysons sur des exemples concrets la pertinence de chacun de ces modèles et leur préservation des états d'équilibre.

16 Le problème de désorption et sa modélisation

On cherche à pomper le gaz de schiste situé dans une fracture souterraine, qui a un volume initial V^0 et une pression P^0. Pour cela, on installe un puits qui va permettre de créer une dépression (comme un appel d'air). La pression à l'entrée du puits est $P^* < P^0$ engendre la dépression et le gaz est évacué vers le haut du puits.



On cherche l'évolution de la pression $P(x,t)$ et du volume $V(x,t)$ du gaz présent dans la fracture. Après plusieurs discussions et changements, le modèle que nous avons retenu est donné par le système d'équations suivant, *redimensionné* (P devient KP):

$$\partial_t V = K \partial_{xx} P \,, \tag{16.1a}$$

$$\partial_t V = k_c \left(\frac{V_L P}{P + K P_L} - V \right) , \tag{16.1b}$$

où K est la perméabilité de la roche constituant la fracture, k_c la constante dite *cinétique*, V_L et P_L les volume et pression de Langmuir, et P la pression.

Il est à noter que l'IFPEN avait déjà simplifié à l'extrême les équations, pour que l'on puisse travailler en une dimension. L'équation (16.1a) sera appelée *équation de diffusion*: elle lie le gradient de pression à la variation

de volume. L'équation (16.1b) sera appelée *équation de relaxation*: elle a été rajoutée par l'IFPEN et correspond à une relaxation d'un modèle plus simple. Lorsque la constante k_c tend vers l'infini, on retrouve bien le modèle de Langmuir:

$$V = \frac{V_L P}{P + P_L}.$$

Nous exigeons de plus des conditions au bord de Dirichlet:

$$\begin{cases} P(x = 0, t) = P_0\,, \\ P(x = L, t) = P_*\,. \end{cases} \tag{16.2}$$

Nous donnons à présent les notations liées à la discrétisation du système d'équations ci-dessus. La fracture est assimilée à un segment $[0, L]$ que l'on subdivise régulièrement avec un pas Δx: on obtient $I+2 \in \mathbb{N}$ noeuds dénotés par $x_i = i\Delta x$ avec $x_0 = 0$ et $x_{I+1} = L$. L'intervalle de temps $[0, T]$ est subdivisé régulièrement avec un pas Δt: on obtient $N \in \mathbb{N}$ pas de temps discrets $t^n = n\Delta t$. On veut écrire un schéma numérique qui calcule $P_i^n \approx P(x_i, t_n)$ et $V_i^n \approx V(x_i, t_n)$, i.e. la pression et le volume en chaque noeud x_i et à chaque temps t_n. Dans toutes nos approches (sections 18.1, 18.2 et 18.3) nous discrétisons l'opérateur ∂_{xx} (laplacien) par des différences finies centrées d'ordre 2, comme spécifié dans la prochaine section.

17 Discrétisation de la partie spatiale

Nous avons décidé de discrétiser $\partial_{xx} P$ par des différences finies centrées d'ordre 2, il s'agit d'une méthode standard de discrétisation du laplacien. On a donc:

$$\partial_{xx} P(x_i, t^n) \approx \frac{1}{\Delta x^2}\big(P_{i-1}^n - 2P_i^n + P_{i+1}^n\big).$$

En tenant compte que, d'après les conditions au bord de Dirichlet (16.2), on a $P(x_0, t^n) = P_0$ et $P(x_{I+1}, t^n) = P_*$, on peut réécrire la discrétisation spatiale sous forme matricielle $A\vec{P}^n$, avec

$$\vec{P}^n = {}^t\left(P_1^n, P_2^n, \ldots, P_{I-1}^n, P_I^n\right)$$

et

$$A = \frac{1}{\Delta x^2}\begin{pmatrix} -2 & 1 & 0 & \cdots & 0 \\ 1 & -2 & 1 & \ddots & \vdots \\ 0 & \ddots & \ddots & \ddots & 0 \\ \vdots & \ddots & 1 & -2 & 1 \\ 0 & \cdots & 0 & 1 & -2 \end{pmatrix}, \tag{17.1}$$

Les conditions au bord seront donc inclues opportunément dans le terme connu de l'équation.

Remarque 17.1. *La matrice $-A$ est une M-matrice car elle est une Z-matrice (tous ses éléments extra- diagonaux sont négatifs) et elle est une P-matrice ($-A$ est symétrique et définie positive). Du fait que $-A$ est une P-matrice on déduit qu'elle est inversible et que $(-A)^{-1}$ a tous ses éléments positifs, ce qui va nous aider à montrer que P reste positive dans le schéma d'ordre 1 en temps dans les sections 18.1 et 18.2. D'autres conditions au bord seraient tout aussi applicables, même si il faut faire attention car, par exemple, si l'on met des conditions au bord de Neumann à la fois en $x = 0$ et en $x = L$, cette méthode des différences finies nous amène à une matrice A non inversible.*

Remarque 17.2. *La matrice A est tridiagonale: on peut donc appliquer l'algorithme de Thomas ([1, section 2.4]) pour résoudre tout système linéaire basé sur A. Ceci nous permet d'avoir une résolution rapide, avec seulement $\mathcal{O}(N)$ opérations, contre $\mathcal{O}(N^3)$ pour une factorisation LU classique.*

18 Schémas d'ordre 1 en temps utilisés

Les schémas numériques présentés vont tous avoir une propriété en commun : ils vont avoir recours à un traitement implicite de l'équation de relaxation (16.1b). Leur différence majeure sera le traitement de l'équation de diffusion (16.1a): par exemple, le premier schéma proposé utilisera un traitement explicite de cette équation.

Rappelons que l'on considère une partition uniforme de l'intervalle temporel $[0, T]$:

$t^0 \leq t^1 \leq \cdots \leq t^{N-1} \leq t^N$, avec $\Delta t = |t^n - t^{n-1}|$ pour tout $n \in \{0, \ldots, N\}$, comme montré dans la Figure 1.

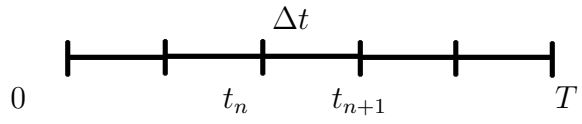


Figure 1: Partition uniforme de l'intervalle temporel $[0, T]$.

Dans cette section on s'intéressera à des schémas d'ordre 1 en temps :

la dérivée temporelle $\partial_t V$ sera toujours approchée par une différence finie antérieure à $V(\cdot, t)$, c'est-à-dire de la manière suivante :

$$\partial_t V(\cdot, t^{n+1}) \equiv \frac{V_i^{n+1} - V_i^n}{\Delta t}. \tag{18.1}$$

18.1 Schéma explicite en espace

Pour l'équation de diffusion, on applique ici un schéma explicite en espace et le schéma d'Euler explicite en temps. Ceci nous donne la discrétisation

suivante de l'équation de diffusion :

$$\frac{V_i^{n+1} - V_i^n}{\Delta t} = \frac{K}{\Delta x^2}\left(P_{i+1}^n - 2P_i^n + P_{i-1}^n\right),$$

dont on extrait la valeur du volume au point x_i, mise à jour au temps t^{n+1} :

$$V_i^{n+1} = V_i^n + \frac{K\Delta t}{\Delta x^2}\left(P_{i+1}^n - 2P_i^n + P_{i-1}^n\right). \tag{18.2}$$

Afin de résoudre (18.2), il faut utiliser les conditions aux bords de Dirichlet (16.2) fournies sur la pression.

On discrétise maintenant l'équation de relaxation avec le schéma d'Euler implicite en temps afin d'obtenir P_i^{n+1} :

$$\frac{V_i^{n+1} - V_i^n}{\Delta t} = k_c\left(\frac{V_L P_i^{n+1}}{P_i^{n+1} + P_L} - V_i^{n+1}\right). \tag{18.3}$$

Cette équation (18.3) nous permet d'obtenir la valeur de P_i^{n+1} en fonction des volumes aux temps t^n et t^{n+1} :

$$P_i^{n+1} = -P_L \frac{V_i^{n+1} - V_i^n + k_c\Delta t V_i^{n+1}}{V_i^{n+1} - V_i^n + k_c\Delta t\left(V_i^{n+1} - V_L\right)}. \tag{18.4}$$

Grâce aux deux équations (18.2) et (18.4), nous avons obtenu un schéma explicite en espace, d'ordre 1 en temps, qui résout le système (16.1).

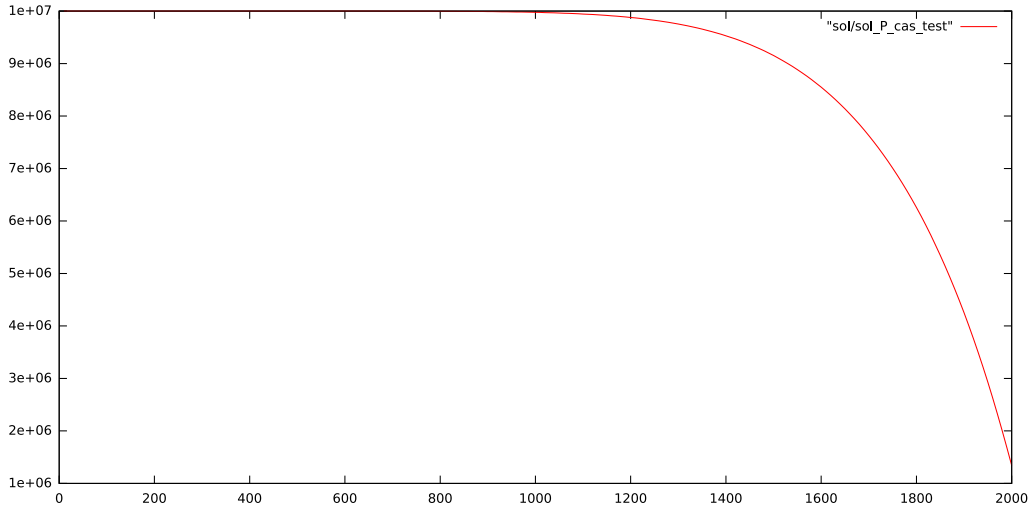


Figure 2: Pression obtenue avec le schéma explicite, pour le cas-test proposé.

Les résultats obtenus (Figure 2 et Figure 3) paraissant concluants, nous avons décidé de nous intéresser à d'autres propriétés du schéma.

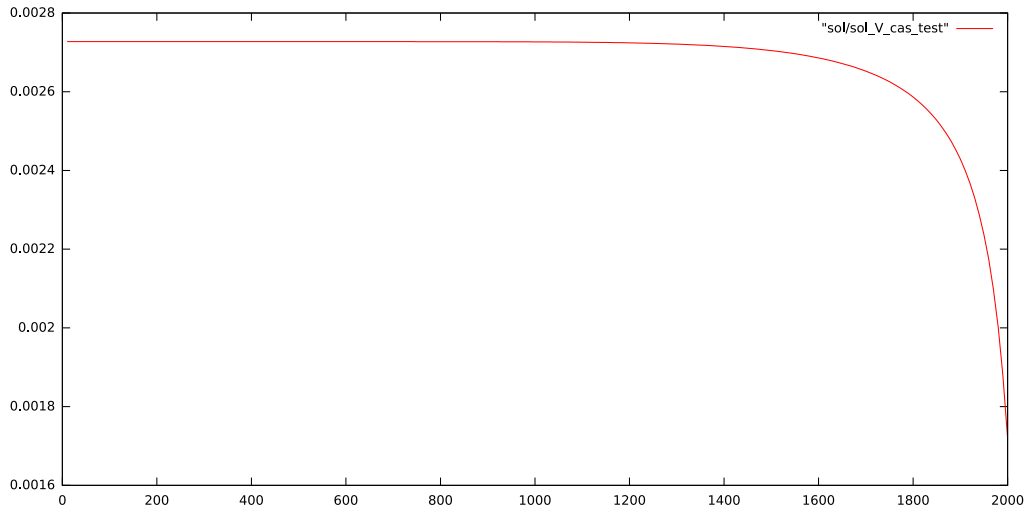


Figure 3: Volume obtenu avec le schéma explicite, pour le cas-test proposé.

- Préserve-t-il les états d'équilibre ?
- Préserve-t-il la positivité de la pression ainsi que les bornes du volume ?

Concernant les états d'équilibre, il faut tout d'abord les déterminer. Un état d'équilibre du système (16.1) est obtenu en annulant toutes les dérivées temporelles. On a donc, en annulant $\partial_t V$ dans (16.1a) et (16.1b) :

$$\partial_{xx} P = 0 \tag{18.5a}$$

$$V = \frac{V_L P}{P + P_L}. \tag{18.5b}$$

(18.5a) donne que la pression est une fonction affine de l'espace. On peut la déterminer point par point en utilisant les conditions aux limites : $P(x_0, \cdot) = P_0$ et $P(x_{I+1}, \cdot) = P_{I+1}$. Des calculs simples donnent finalement

$$P_i = P_0 - (P_0 - P_{I+1}) \frac{i}{I+1}. \tag{18.6}$$

Grâce à cette expression de P_i, le volume à l'équilibre est défini sur tout le domaine par (18.5b) :

$$V_i = \frac{V_L P_i}{P_i + P_L}. \tag{18.7}$$

Nous pouvons maintenant étudier le schéma proposé afin de déterminer s'il est *well-balanced*, i.e. s'il préserve ces états d'équilibre. Pour ce faire, on suppose que le volume et la pression sont à l'équilibre au temps t^n, et on regarde s'ils y sont toujours au temps t^{n+1}. On voit aisément que, si la pression est affine, (18.2) donne immédiatement que $V_i^{n+1} = V_i^n$. Ensuite, (18.4) devient

$$P_i^{n+1} = \frac{-P_L V_i^n}{V_i^n - V_L}, \tag{18.8}$$

ce qui n'est autre qu'une réécriture de (18.7). On a donc aussi $P_i^{n+1} = P_i^n$, et le schéma est well-balanced. Numériquement, on le vérifie en prenant une donnée initiale à l'équilibre et en remarquant que toutes les itérations suivantes restent à l'équilibre. On peut aussi s'intéresser à la perturbation d'un état d'équilibre, en prenant en donnée initiale un état proche d'un équilibre, et en laissant évoluer cet état : à temps assez long, il devrait revenir à l'équilibre. Ce résultat est vérifié Figure 4.

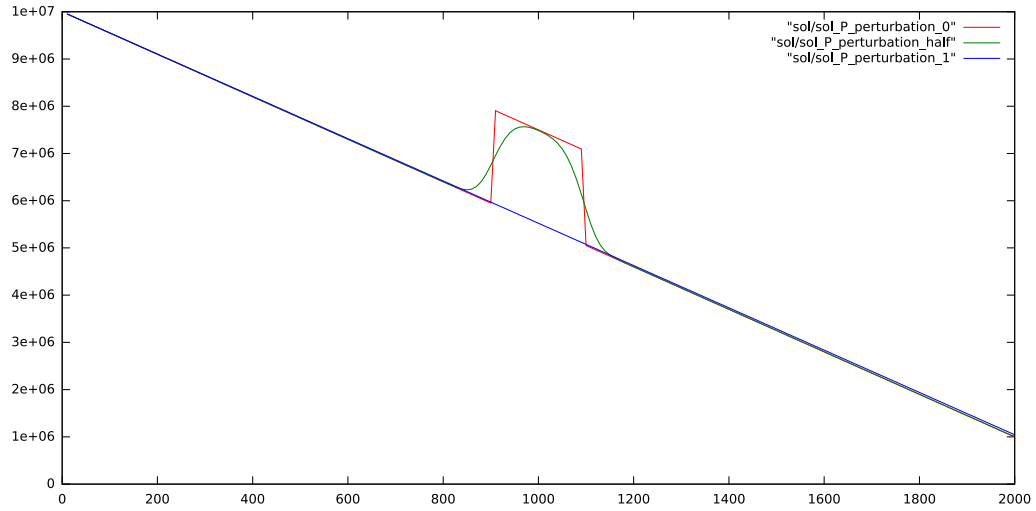


Figure 4: La courbe rouge est la pression pour l'équilibre perturbé, condition initiale imposée. La courbe verte montre l'évolution de cette pression après quelques pas de temps : on remarque que la perturbation commence à s'aplatir et se propager dans les deux directions. La courbe bleue représente la pression après un temps de simulation assez long : on voit qu'elle tend vers l'équilibre non perturbé, ce qui valide ce cas-test de préservation des états d'équilibre.

On s'intéresse maintenant à la préservation des bornes de la pression et du volume : on rappelle qu'on veut avoir $P > 0$ et $0 < V < V_L$.

18.2 Schéma implicite en espace

On s'intéresse ici à un schéma implicite en espace pour l'équation de diffusion. Dans ce cas, pour obtenir la pression à l'instant t_{n+1} à partir de l'équation de diffusion, on a besoin d'avoir le volume à l'instant t^n et t^{n+1}. Pour cette raison on choisit tout d'abord d'obtenir V^{n+1} à partir de l'équation de relaxation. Pour cela on a recours à une discrétisation semi-implicite en temps (le volume discrétisé de façon implicite et la pression de façon explicite) comme suit :

$$\frac{V_i^{n+1} - V_i^n}{\Delta t} = k_c \left(\frac{V_L P_i^n}{P_i^n + P_L} - V_i^{n+1} \right). \tag{18.9}$$

On extrait de (18.9) la valeur de V_i^{n+1} :

$$V_i^{n+1} = \frac{1}{1 + k_c \Delta t} \left(V_i^n + k_c \Delta t \frac{V_L P_i^n}{P_i^n + P_L} \right), \tag{18.10}$$

ce qui nous permet d'aller résoudre l'équation de diffusion de façon implicite en espace :

$$\frac{V_i^{n+1} - V_i^n}{\Delta t} = \frac{K}{\Delta x^2} \left(P_{i+1}^{n+1} - 2P_i^{n+1} + P_{i-1}^{n+1} \right). \tag{18.11}$$

En utilisant les notations de la section 17, on peut exprimer (18.11) de manière compacte sur tout l'espace :

$$-A\,\vec{P}^{n+1} = \vec{b}^{n+1}, \text{ où} \tag{18.12}$$

- A est la matrice (17.1);
- $\vec{P}^{n+1} = {}^t\left(P_1^{n+1}, P_2^{n+1}, \ldots, P_{I-1}^{n+1}, P_I^{n+1}\right)$;
- $\vec{b}^{n+1} = \frac{\Delta x^2}{K \Delta t}\left(\vec{V}^n - \vec{V}^{n+1}\right) + {}^t\left(P_0^{n+1}, 0, \ldots, 0, P_{I+1}^{n+1}\right)$, avec $\vec{V}^n = {}^t\left(V_1^n, V_2^n, \ldots, V_{I-1}^n, V_I^n\right)$ pour tout n.

La solution $\vec{P}^{n+1}$ est obtenue en résolvant ce système linéaire.

On peut faire quelque remarques sur la *well-balanced property* et la positivité.

- Ce schéma ne préserve pas les états d'équilibre: si on suppose que le volume et la pression sont à l'équilibre au temps t^n, ils ne le seront pas au temps t^{n+1}. On suppose le volume et la pression respectivement comme dans (18.7) et (18.6), on constate qu'au temps t^{n+1} on a bien pour le volume

  $$V_i^{n+1} = \frac{V_L P_i}{P_i + P_L}, \tag{18.13}$$

  or pour la pression

  $$\vec{P}^{n+1} = {}^t\left(P_0^{n+1}, 0, \ldots, 0, P_{I+1}^{n+1}\right). \tag{18.14}$$

  Ce qui est en contradiction avec la demande d'avoir, aussi au temps t^{n+1}, une pression discrète donnée par (18.6).

- Concernant la positivité du schéma, supposons P^n et V^n positifs. Puisque les coefficients de l'équation (18.10) sont tous positifs, le volume $\vec{V}^{n+1}$ sera positif. Ensuite, comme $-A$ est une P-matrice et le volume décroissant en temps de la (18.12) suit que $\vec{P}^{n+1}$ sera positive.

18.3 Schéma implicite en espace qui utilise un couplage des équations

Au vu des résultats non concluants du schéma implicite précédent, nous avons utilisé une discrétisation semi-implicite en pression de l'équation de relaxation :

$$\frac{V_i^{n+1} - V_i^n}{\Delta t} = k_c \left(\frac{V_L P_i^{n+1}}{P_i^n + P_L} - V_i^{n+1} \right). \tag{18.15}$$

Cette équation nous donne une expression de V_i^{n+1} en fonction de P_i^{n+1} :

$$V_i^{n+1} = \frac{1}{1 + k_c \Delta t} \left(V_i^n + k_c \Delta t \frac{V_L P_i^{n+1}}{P_i^n + P_L} \right). \tag{18.16}$$

Nous pouvons injecter (18.16) dans la discrétisation implicite en espace (18.11) de l'équation de diffusion. Ceci nous donne une équation du type (18.12) à résoudre pour obtenir P_i^{n+1}. On a donc

$$\widetilde{A}^n \vec{P}^{n+1} = \widetilde{b}^n, \text{ où} \tag{18.17}$$

- $\widetilde{A}^n = A - \text{diag}\left(\left(\frac{\Delta x^2}{K \Delta t} \frac{k_c \Delta t}{1 + k_c \Delta t} \frac{V_L}{P_i^n + P_L} \right)_{i \in [1,N]} \right)$;
- $\vec{P}^{n+1} = {}^t \left(P_1^{n+1}, P_2^{n+1}, \ldots, P_{I-1}^{n+1}, P_I^{n+1} \right)$;
- $\widetilde{b}^n = \frac{\Delta x^2}{K \Delta t} \frac{k_c \Delta t}{1 + k_c \Delta t}{}^t \left(-V_1^n, -V_2^n, \ldots, -V_{I-1}^n, -V_I^n \right) + {}^t \left(-P_0, 0, \ldots, 0, -P_N \right)$.

Résoudre le système linéaire (18.17) nous donne la valeur de P_i^{n+1} pour chaque nœud x_i, donc on déduit la valeur de V_i^{n+1} en appliquant la formule (18.16) à tous les nœuds x_i.

Ces résultats semblent meilleurs que ceux obtenus avec le schéma implicite non couplé, mais ne sont tout de même pas concluants. On remarque que pression et volume sont presque uniformes sur le domaine, sauf très près des bords. Ceci peut s'expliquer formellement en regardant de plus près le système (18.17). En effet, à cause des divisions par K (qui est très petit, de l'ordre de 10^{-15} m^2), la diagonale de $\widetilde{A}^n$ va être très grande devant les termes extra-diagonaux. De même, toutes les composantes de b^n va être grandes : en effet, les conditions aux limites P_0 et P_{N+1} sont de l'ordre de $\sqrt{K}$, et n'ont donc que peu d'impact comparé au reste du terme source. On a donc un système presque diagonal à résoudre : il y aura donc peu d'interactions entre les différentes cellules, ce qui explique le palier de pression (et donc de volume) vers le milieu du domaine.

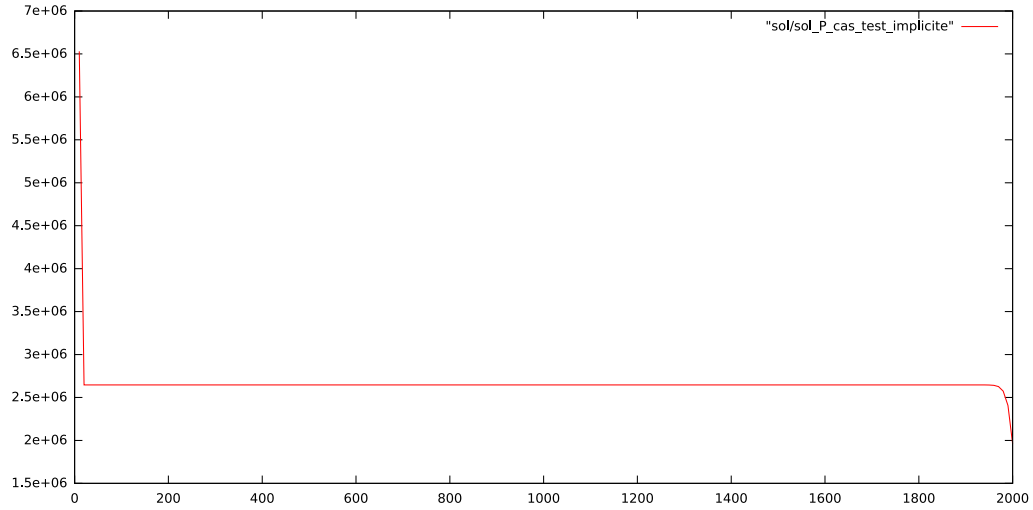


Figure 5: Pression obtenue avec le schéma couplé, pour le cas-test proposé.

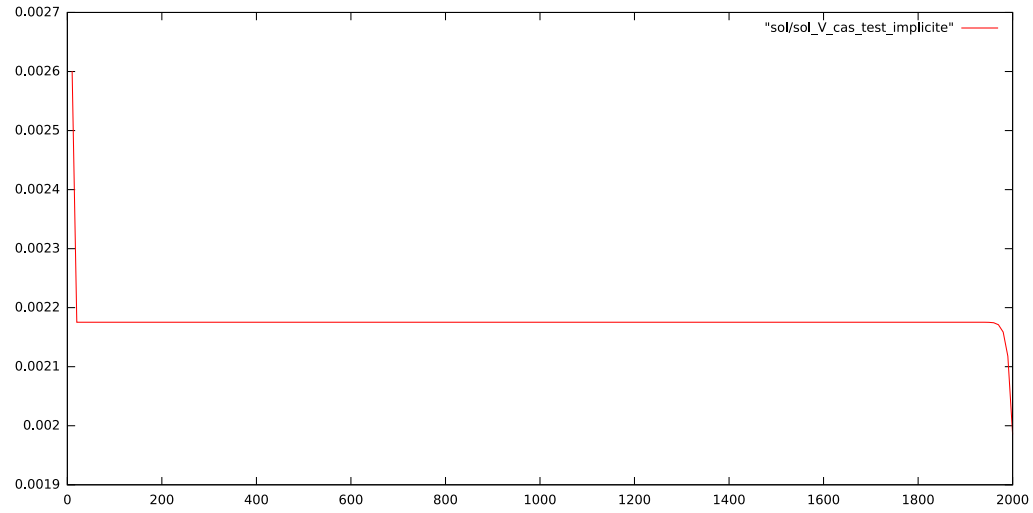


Figure 6: Pression obtenue avec le schéma couplé, pour le cas-test proposé.

19 Perspectives pour un schéma numérique d'ordre 2 en temps

19.1 Le schéma RK2-TVD

Supposons que l'on dispose d'un schéma d'ordre 1 explicite en temps, stable pour un pas de temps satisfaisant $\Delta t \leq \Delta t_c$. Partant d'un schéma d'ordre 1 explicite en temps, les auteurs de [2] proposent des schémas d'ordre 2 et 3 en temps, basés sur des méthodes de Runge-Kutta, et telle que la stabilité en temps devienne $\Delta t \leq c\Delta t_c$, avec $c < 1$.

Notons $u : t \in I \mapsto (V(t), P(t)) \in \mathbb{R}^2$ la fonction vectorielle donnant le volume et la pression au temps t. Notons $\widetilde{S}_{\Delta t}(u^n)$ le résultat de notre schéma numérique explicite (voir section 18.1) appliqué à la donnée initiale u^n et avec un pas de temps Δt; autrement dit $u^{n+1} = \widetilde{S}_{\Delta t}(u^n)$ dans ce schéma.

Le schéma d'ordre 2 proposé dans [2, proposition 3.1] est de la forme:

$$\begin{aligned} u^* &= u^n + \Delta t \widetilde{S}_{\Delta t}(u^n), \\ u^{n+1} &= \frac{1}{2}u^n + \frac{1}{2}u^* + \frac{1}{2}\widetilde{S}_{\Delta t}(u^*); \end{aligned}$$

et le schéma d'ordre 3 proposé dans [2, proposition 3.1] est de la forme:

$$\begin{aligned} u^* &= u^n + \Delta t \widetilde{S}_{\Delta t}(u^n), \\ u^{**} &= \frac{3}{4}u^n + \frac{1}{4}u^* + \frac{1}{4}\widetilde{S}_{\Delta t}(u^*), \\ u^{n+1} &= \frac{1}{3}u^n + \frac{2}{3}u^{**} + \frac{2}{3}\widetilde{S}_{\Delta t}(u^{**}). \end{aligned}$$

Ces deux schémas sont optimaux au sens où $c = 1$. De plus, ils préservent la monotonie dès que $\widetilde{S}_{\Delta t}$ la préserve. D'après [2, proposition 3.1], à partir de l'ordre 4, il n'est plus certain que cette propriété soit encore vérifiée.

References

[1] Press, WH; Teukolsky, SA; Vetterling, WT; Flannery, BP; *Numerical Recipes: The Art of Scientific Computing*, troisième édition, Cambridge University Press, 2007.

[2] Gottlieb, S.; Shu, CW; *Total variation diminishing Runge-Kutta schemes*, Math. Comp., vol. 67, pages 73–85, 1998.

Part IV

Annexe : Activité de diffusion

20 Le jeu Set

Nous reportons ici un article de vulgarisation paru dans la rubrique "l'objet du mois" du site Image des mathématiques, rubrique consacrée à la présentation d'objets mathématiques :
" Le monde mathématique est peuplé d'objets allant du très concret au très abstrait. Dans cette rubrique, on se propose d'en présenter quelques-uns parmi les plus importants, beaux, utiles ou étonnants. Même lorsque leur découverte est ancienne, ils sont toujours d'actualité dans la recherche comme (contre-)exemples, comme outils, ou comme source d'inspiration."
http://images.math.cnrs.fr/-Objet-du-mois-.html

Objet du mois *(-Objet-du-mois-.html)*

LE JEU SET

Piste bleue *(spip.php?page=mot&id_mot=21)* *le 5 mai 2013* - Rédigé par Pierre Jalinière

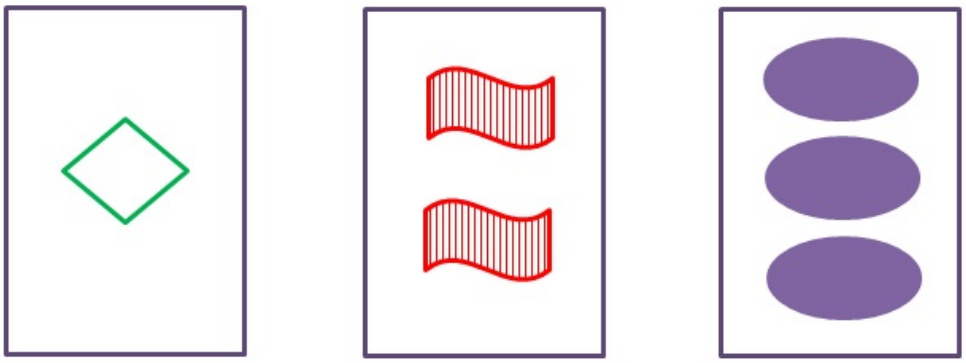
(_Jaliniere-Pierre_.html)

Venu d'outre-Atlantique, Set est un jeu de carte qui se joue à plusieurs et qui consiste pour chaque joueur à identifier le plus vite possible des familles de cartes compatibles. C'est aussi un jeu qui permet de se poser des questions combinatoires, algébriques, algorithmiques ou géométriques ; certaines restent ouvertes.
Nous décrivons le jeu Set, examinons certaines de ses questions combinatoires puis les traduisons en termes spatiaux. On peut espérer tout lire avec un niveau terminale. L'occasion de pratiquer déjà de belles mathématiques ! [1 *(#nb1)*].

Ici, un Set vivant.

Le jeu Set

Set se joue avec des cartes originales. Sur chaque carte on trouve d'une à trois formes identiques munies d'une couleur et d'un mode de remplissage. Les formes sont : Vague, Losange, Ovale. Les couleurs : Rouge, Vert et Violet. Les remplissages : Hachuré, Plein, Vide. Par exemple, ici l'on a « un losange vert vide », « deux vagues hachurées rouges » et « trois ovales pleins violets ».



Il y a exactement une carte pour chaque famille de caractéristiques possibles ce qui permet de répondre à la question : **Combien compte-t-on de cartes dans un jeu Set ?**

Comme il y a trois valeurs possibles pour chacune des quatre caractéristiques on trouve un total de $3^4 = 81$ cartes à jouer.

Un Set est une collection de trois cartes dont les quatre caractéristiques sont soit différentes, soit identiques. Ainsi la famille de trois cartes donnée en exemple est un Set. Pour faire un Set, les trois cartes doivent présenter quatre critères :

- être un Set pour les nombres. Ceci signifie que chaque carte contient le même nombre de figures, soit une, deux, ou trois exactement, un autre cas courant advient quand les trois cartes portent des nombres tous différents. C'est-à-dire pour un Set en nombre contiennent respectivement une, deux et trois figures.
- être un Set en figures : il s'agit maintenant d'avoir le même type de figure sur chaque carte ou les trois types de figures représentés (un type par carte), différent pour chaque carte.
- être un Set en couleurs.
- être un Set en remplissages.

Etre un Set, c'est être ces quatre sortes de Set à la fois. Remarquons que chaque carte étant unique, pour l'un de ces critères au moins, la caractéristique diffère d'une carte à l'autre (par exemple, pour un Set en figure on aura vague, losange, ovale).

Comment joue-t-on à Set ?

Le jeu commence en disposant douze cartes devant les joueurs. Le premier qui trouve un Set parmi ces douze cartes collecte les trois cartes qui le constituent. On remet sur la table trois nouvelles cartes tirées du paquet et le jeu continue jusqu'à ce qu'il n'y ait plus de carte à disposer sur la table. Le gagnant est celui qui a trouvé le plus de Set pendant la partie.

La principale faiblesse de ces règles est qu'il se peut qu'il n'y ait pas de Set parmi les douze cartes disposées devant les joueurs (Un problème similaire se pose pour le jeu Dobble par exemple, voir ici *(Dobble-et-la-geometrie-finie.html)*). Quand les joueurs tombent d'accord, on sort du paquet trois nouvelles cartes qui viennent rejoindre celles déjà visibles. Si l'un des joueurs trouve un Set parmi ces quinze cartes, il s'en empare sans extraire trois nouvelles cartes du paquet. Le jeu continue. S'il n'y a toujours aucun Set, on tire trois nouvelles cartes et ainsi de suite jusqu'à ce qu'un des joueurs identifie un Set.

La partie se termine quand il n'y a plus de cartes dans le paquet et que les cartes sur la table ne forment aucun Set. Très rarement, lors de la partie, toutes les cartes ont été utilisées, s'intégrant toutes dans l'un des Set ramassés par les joueurs. La fréquence de ces jeux « complets » est une question qui reste ouverte. Le lecteur s'il trouve la réponse, est chaleureusement invité à la transmettre au comité éditorial. Il faut un peu de pratique pour identifier les Set. Un moyen sûr d'en trouver s'appuie sur la règle suivante :

Pour deux cartes arbitraires, il n'existe qu'une unique troisième carte qui les complète pour faire des trois un Set.

En effet, pour chaque caractéristique, deux cartes arbitraires sont identiques ou différentes. Comme il n'y a que trois valeurs pour chacune de ces caractéristiques, la troisième carte est uniquement déterminée à partir des deux premières.

Cette règle permet de répondre à au moins deux questions :

(1) : Quelle est la probabilité, tirant trois cartes au hasard, de former un Set ?

Le jeu comporte 81 cartes et deux cartes parmi les trois sont arbitraires, celles-ci prisent ensemble, la troisième est unique parmi les 79 restantes. Soit une probabilité de 1/79 que la combinaison tirée soit un Set.

(2) : Combien le jeu comporte-t-il de Set ?

Il y a 81 choix possibles pour la première carte et 80 choix possibles par la seconde. Ces deux cartes déterminent de manière unique la troisième du Set. L'ordre des cartes ne compte pas, on doit donc diviser 81× 80 par 3 !=3×2=6. Soit exactement 1080 Sets possibles avec les cartes du jeu.

(3) : Quels sont les Set les plus faciles à repérer ?

On compte quatre sortes de Set distincts. On peut les classer en fonction du nombre de caractéristiques partagées par les cartes : Aucune, une, deux ou trois. Celles en partageant trois, ce qu'on nomme ici les trois-Set, sont visuellement plus faciles à identifier. Par exemple, voici ce que peut être un trois-Set : « un, plein, rouge, vague », « deux, plein, rouge, vague », « trois, plein, rouge, vague ». Un Set dont toutes les caractéristiques diffèrent, les différents-Set, sont les plus difficiles à remarquer. C'est un Set de cette espèce qui est représenté plus haut. On peut alors se poser la question :

(4) : Parmi tous les Set possibles quelle est la probabilité de chacun de ces types ?

En raisonnant de la même façon que pour la question (2), on trouve pour les trois-Set, exactement 108 possibilités parmi les 1080 choix possibles de Set. Soit 10%. Pour les deux-Set, 324, soit 30%. Pour les un-Set, 432, soit 40%. Enfin pour les différent-Set, 216, autrement dit, 20%.

On peut se poser beaucoup de questions combinatoires concernant Set. Et nous n'avons qu'effleuré ce qu'on peut en dire. Un autre aspect du jeu, plus géométrique, donne un sens à la notion de Set et permet d'identifier les cartes à des points dans un certain espace. Voici comment s'y prendre.

Set et sa géométrie

L'espace sur lequel nous allons situer les cartes est fini. C'est-à-dire qu'il ne contient qu'un nombre de points fini. On le construit avec autant de dimensions qu'il y a de caractéristiques pour chaque carte, soit 4. Il y a donc une dimension pour le nombre de figures, une pour leur couleur, une pour leur forme ainsi qu'une pour ce qui les remplit. En mathématiques un tel espace muni d'une géométrie adéquate existe bien. On peut y faire de la géométrie comme à l'habitude : par exemple deux points pris au hasard, définissent une unique droite. Mais ici tout est plus simple, en effet une droite ne contient que 3 points, un plan 9, un hyperplan (c'est-à-dire notre espace de dimension trois plongé dans un espace de dimension quatre) 27, et l'espace tout entier… 81, soit le nombre exact de cartes que contient le jeu Set.

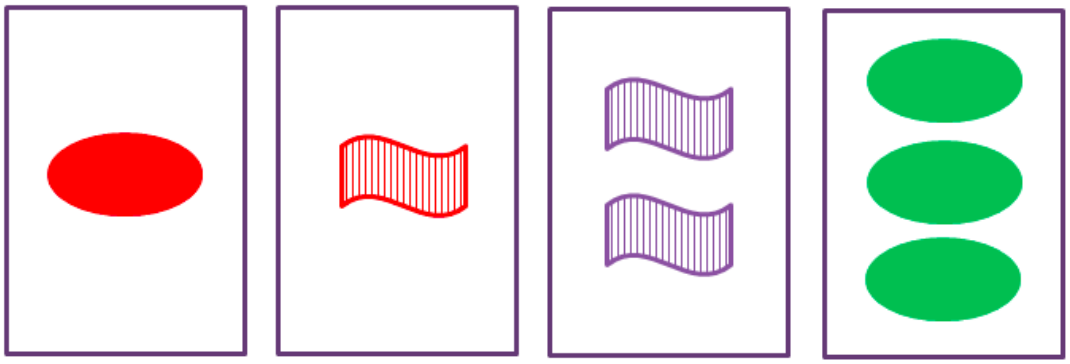
Une carte s'identifie à la donnée d'un point dont les coordonnées sont déterminées par ses caractéristiques et réciproquement, tout point de cet espace détermine une unique carte.

Il est très facile dans cet espace de définir ce qu'est un Set : c'est simplement une droite, en d'autres termes, les trois cartes d'un Set déterminent trois points alignés. Comme en géométrie, on retrouve la règle selon laquelle par deux points passe une et une seule droite : avec deux cartes, seule une troisième permet de les compléter en un Set. De même, un plan se détermine uniquement par la donnée de trois points non colinéaires, ou par la donnée d'une droite et d'un point distinct, ou par la donnée de deux droites

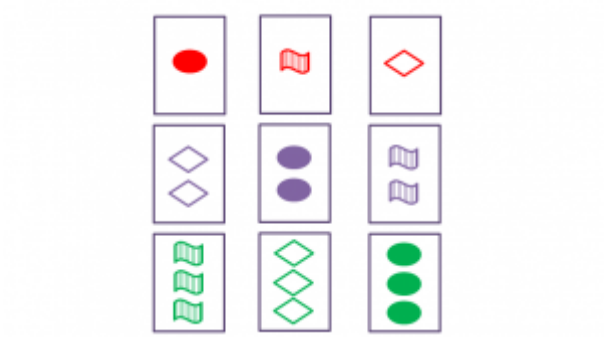
parallèles ou de deux droites qui s'intersectent. Toutes ces assertions restent valables quand elles s'appliquent à Set. Tirons par exemple trois cartes « non colinéaires » puisqu'elles ne forment pas une droite, elles ne forment pas un Set. Celles-ci définissent donc un plan unique. Plan qui se reconstitue comme suit : On rajoute à cette collection une carte telle qu'avec deux des trois précédentes, l'ensemble forme un Set. Et l'on recommence le tirage en suivant la même règle : chaque nouvelle carte tirée doit former un Set, une droite, avec deux des cartes déjà précédemment tirées. En tout, l'on obtiendra exactement neuf cartes. Ces neuf cartes réalisent le plan qu'on a défini en usant des trois premières. Les parties qui suivent, plus difficile, peuvent croit-on, avec un peu d'effort, espérées être lu dès le niveau terminale scientifique.

Planète, variante et définition

Le but est d'introduire une variante du jeu Set, on ne cherche plus à trouver parmi douze cartes trois d'entre elles alignées (autrement dit un Set), mais quatre définissant ensemble un unique plan, c'est-à-dire quatre cartes coplanaires. Quatre points étant pris au hasard, quels sont les cas possibles en géométrie classique ? Le premier, c'est que ces quatre points soient alignés. Un tel cas ne peut se produire pour Set puisqu'on a vu que toute droite contient exactement trois points. Si l'on tire une quatrième carte, un quatrième point, ce dernier nécessairement se trouve à l'extérieur de la droite. Ensemble, ils définissent un plan. C'est l'un des deux cas qu'on appellera Planète. L'autre correspond à quatre points définissant deux droites qui s'intersectent. En langage Set, cela signifie que deux à deux, quatre cartes définissent deux Set qui se complètent par la même troisième carte. Voici un exemple de quatre cartes Planète répondant à cette condition :



Ici, le plan complet défini par ces quatre mêmes cartes :



Qu'en déduit-on sur le jeu ? Il y a plus de combinaisons gagnantes car dès qu'on a un Set n'importe quelle quatrième carte définit une Planète. La probabilité tirant quatre cartes au hasard de former une Planète est plus grande que la seule probabilité de former un Set tirant trois d'entre elles du jeu complet :

(5) : Quelle est la probabilité tirant quatre cartes de former une Planète ?

Deux cas sont possibles, soit la Planète contient un Set, soit elle n'en contient pas. La probabilité de tirer un Set dès les 3 premières cartes est comme on l'a vu de 1/79. La probabilité de n'en pas tirer, l'événement contraire, est donc de 78/79. Or trois cartes qui ne forment pas un Set définissent un unique plan. Six autres cartes appartiennent à ce même plan, ainsi la probabilité que la quatrième carte tirée forme une Planète avec les trois précédentes est exactement de 6/78, 6 cartes possibles parmi les 78 restantes. Soit une probabilité de tirer une Planète de : $1/79 + (78/79) \times (6/78) = 7/79$. Il y a donc sept fois plus de chances de tirer une planète qu'un simple Set. Ces chances importantes induisent la question suivante :

(6) : A partir de combien de cartes tirées est-on sûr de disposer d'une planète ?

Elle fait l'objet de la prochaine partie.

Set, Planète à l'épreuve du jeu

Davis et Maclagan [2 *(#nb2)*] ont montré que pour un jeu de Set à trois dimensions (par exemple si l'on décide de ne jouer qu'avec des cartes de couleur rouge), on peut tirer jusqu'à 9 cartes sans Set. Mais 10 cartes tirées contiennent toujours un Set. Pour le jeu complet, soit 81 cartes, on peut tirer jusqu'à 20 cartes sans qu'il y ait de Set, la 21ème permettra toujours d'en former un. Pour les Planètes nous étudierons d'abord le cas de la dimension 3.

Planète à trois dimensions

On peut tirer jusqu'à cinq cartes rouges sans Planète :

On prouve en deux temps que cinq telles cartes ne contiennent pas de Planète. D'abord, on s'assure qu'elles ne contiennent pas de Set. Ensuite, pour un couple de cartes données, on donne la troisième carte qui fait du trio complet un Set. Pour s'assurer qu'il n'y a pas de Planète, il suffit de vérifier que ces troisièmes cartes déduites de tout couple sont bien différentes. Le nombre de couples correspond au choix de deux cartes parmi cinq. C'est le nombre de combinaison de 2 éléments pris dans un ensemble à 5 éléments. Ce nombre en mathématiques est noté de la manière suivante :

$$\binom{5}{2} = 10$$

Soit donc 10 couples de cartes à vérifier. Il est clair qu'aucune des troisièmes cartes qui s'en déduisent ne sont les mêmes : on ne peut pas trouver de Planète parmi ces cinq cartes.

(7) : Avec sept cartes peut-on toujours former une Planète ?

La réponse est oui, voici la preuve : Supposons qu'on dispose de sept cartes sans Planète. Entre autres, elles ne forment pas de Set, et pour tout couple de cartes, les troisièmes qui forment un Set avec un tel couple doivent être toutes distinctes. On compte de la même façon : $\binom{7}{2} = 21$ choix de couples de cartes possibles. S'il y avait autant de troisièmes cartes de Set qu'il y a de couples on compterait en tout 21+7=28 cartes rouges et le jeu n'en compte que 27. C'est une contradiction qui conclut la preuve.

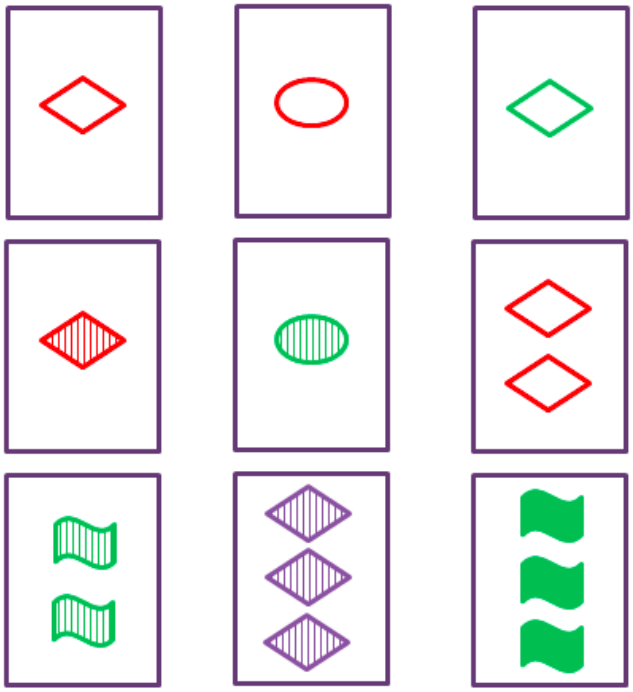
Reste le cas où l'on tire six cartes. Le groupe de travail du Math Teachers' circle a mis à l'épreuve par ordinateur tous les sextuplés possibles et la réponse est la suivante : Avec six cartes, on peut toujours former une Planète au moins.

Planète en dimension 4

La même question se pose quand on décide de ne plus se restreindre aux seules cartes rouges. C'est l'objet de la dernière question de la partie précédente reformulée ici :

(8) : Le jeu pris en entier combien de cartes au plus peut-on tirer sans former une Planète ?

L'argument utilisé en dimension 3 s'adapte dans ce cas pour treize cartes. Si 13 cartes, soit 13 points ne contiennent aucun Set, elles déterminent $\binom{13}{2} = 78$ droites toutes distinctes. Si de ces 13 points l'on ne peut extraire aucune Planète, cela veut dire que le jeu compte au moins 78+13 =91 points or on a vu plus tôt que Set contient exactement 81 cartes. Qu'en est-il pour 12 cartes ? Le même calcul aboutit au fait que le jeu doit contenir au moins 78 cartes, ce qui n'a rien d'absurde, dans ce cas cette méthode ne permet pas de conclure. Remarquons d'abord qu'il existe bien des collections de neuf cartes sans Planète, voici un exemple :



On laisse au plus patient des lecteurs la preuve que neuf telles cartes ne contiennent ni Set ni Planète, il faut vérifier que, pour tout couple de cartes, les seules troisièmes qui s'en déduisent formant des trois un Set sont distinctes cela pour tout couple. On compte en

tout trente-six tels couples. Un programme informatique a montré qu'avec dix cartes, on peut toujours former une Planète. Ce même programme permet de déterminer la probabilité de ne pas tirer de Planète parmi neuf cartes. Celle-ci est de : 11664/222981055≅0,0000523093. Soit, à peu près, une chance sur 19117 de tirer neuf cartes sans Planète.

Il existe une propriété possédée par tout ensemble de neuf cartes sans Planète ni Set, ces neuf cartes forment alors ce qu'on appelle un ET.

ET

De la même façon que pour un Set, on décompose la définition d'un ET en quatre étapes. ET en couleur, en nombre, en forme, en remplissage. Neuf cartes étant données, elles forment un ET en couleur, si l'on peut les rassembler de telles sortes qu'elles forment trois Set en couleur. S'il en est de même pour chaque caractéristique, on parle d'un ET. Les neuf cartes représentées plus haut en donnent un exemple.

On ne connait pas de preuve naïve assurant que neuf cartes ne formant ni Set ni Planète forment toujours un ET, mais un programme exhaustif a montré que c'était bien toujours le cas. D'ailleurs remarquons que la réciproque est fausse. Il existe beaucoup de ET contenant des Set ou des Planètes. Voici deux questions naturelles sur ET :

Montrer que pour huit cartes quelconques données, il n'en existe qu'une supplémentaire telle que les neuf ensemble forment un ET.

Quelle est la probabilité tirant neuf cartes au hasard d'obtenir un ET ?

Cela dit, on peut mettre au point un nouveau jeu s'appuyant sur ces deux nouveaux objets : ET et Planète. La dernière partie en définit les règles.

Planète, le jeu

On pose neuf cartes sur la table. Le but du jeu est d'y trouver Set, Planète ou ET. Dès qu'un joueur a trouvé l'une de ces combinaisons, il la montre et la retire du jeu. On tire du paquet autant de cartes que celles récupérées. Le jeu continue jusqu'à ce qu'il n'y ait plus assez de cartes pour qu'on puisse identifier parmi celles restantes ni Set, ni Planète, ni ET. Le gagnant est celui qui dispose du plus de cartes à la fin du jeu.

Dégageons deux avantages à jouer de cette façon.

D'une part, il n'est plus nécessaire de tirer du paquet plus de neuf cartes, en effet comme on l'a dit, neuf cartes qui ne contiennent ni Set, ni Planète forment toujours un ET. Ainsi quoiqu'il arrive et jusqu'à l'avant-dernier tirage, on dispose d'exactement neuf cartes sur la

table. D'autre part, le jeu va beaucoup moins vite que Set, parce que le gagnant est celui disposant du plus de cartes à la fin de la partie. On a tout intérêt à chercher en premier lieu des ET ou des Planètes plutôt que de simples Set. La quête peut s'avérer chronophage.... A conseiller donc pour les longues soirées d'hiver.

Conclusion

Le jeu Set recèle bien des trésors, la géométrie, l'algorithmique, sont deux méthodes qui permettent ici d'en percer certains secrets. Des questions restent ouvertes, d'autres cachées sont peut-être à découvrir. Qu'en est-il par exemple des cartes toutes inscrites dans un espace de dimension trois ? Comment déterminer que cinq cartes sont cospatiales ? Quelle est la probabilité de tirer cinq telles cartes ? Une autre approche consiste à changer les cartes elle même, augmenter par exemple le nombre de caractéristiques. La question de savoir combien de cartes l'on peut alors tirer sans former de Set est partiellement résolue dans l'article de T. Tao ici *(http://oeis.org/A090245)*. Le sujet n'est pas épuisé et le lecteur trouvera sans mal, qu'il soit joueur ou pas, des combinaisons nouvelles, pour autant de nouveaux jeux.

Post-scriptum :

Remerciements à Ariane Mézard sans laquelle cet article n'existerait pas, ainsi qu'aux relecteurs dont les noms ou pseudonymes suivent : Serge Cantat, Damien Gaboriau, Cidrolin, TheBarber, Sébastien Martinez et Nicolas Chatal.

NOTES

[1 *(#nh1)*] Cet article est une transcription de celui rédigé par Mark Baker, Jane Beltran, Jason Buell, Brian Conrey, Tom Davis, Brianna Donaldson, Jeanne Detorre-Ozeki, Leila Dibble, Tom Freeman, Robert Hammie, Julie Montgomery, Avery Pickford et Justine Wong au sein du Math Teacher's Circle [[Le Math Teacher's Circle est une communauté de mathématiciens et d'enseignants américains du secondaire. Elle se réunit régulièrement, et travaille sur des problèmes ouverts de Mathématiques élémentaires. Les auteurs de l'article traduit ici en font partie. (voir ici *(http://www.mathteacherscircle.org.)*)

[2 *(#nh2)*] B. Lent Davis et D. Maclagan, The game Set, Math Intelligencer 25 (2003), no. 3, 3340 ; (voir ici *(http://www.math.rutgers.edu/maclagan/papers/set.pdf)*)

Pierre Jalinière
Institut de Mathématiques de Jussieu - Paris Rive Gauche
Université Pierre et Marie Curie
5 Place Jussieu
75005 Paris